A RAND NOTE

INTELLIGENCE CONSTRAINTS OF THE 1970s AND DOMESTIC TERRORISM: VOL. II, A SURVEY OF LEGAL, LEGISLATIVE, AND ADMINISTRATIVE CONSTRAINTS

Marvin M. Lavin

December 1982

N-1902-DOJ

Prepared for

The U.S. Department of Justice

Rand
SANTA MONICA, CA. 90406

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
DEC 1982		**00-00-1982 to 00-00-1982**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Intelligence Constraints of the 1970s and Domestic Terrorism: Vol. II, A Survey of Legal, Legislative, and Administrative Constraints	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Rand Corporation,1776 Main Street,PO Box 2138,Santa Monica,CA,90407-2138**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**182**	

Prepared under Grant Number 70-NI-AX-0108 from the U.S. Department of Justice. Points of view or opinions stated in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Published by The Rand Corporation

A RAND NOTE

INTELLIGENCE CONSTRAINTS OF THE 1970s AND DOMESTIC TERRORISM: VOL. II, A SURVEY OF LEGAL, LEGISLATIVE, AND ADMINISTRATIVE CONSTRAINTS

Marvin M. Lavin

December 1982

N-1902-DOJ

Prepared for

The U.S. Department of Justice

Rand
SANTA MONICA, CA. 90406

PREFACE

This Note presents a selective survey of legal and administrative regulatory constraints on the collection, maintenance, use, and dissemination of information pertaining to domestic security during the 1970s. The study considers only domestic intelligence concerning domestic terrorism; it does not consider foreign or international intelligence and counterintelligence.

Because of limited access to investigators' manuals, we were not able to ascertain how policy and legal constraints have been expressed as operational rules for initiating, conducting, and terminating surveillance and other investigatory activities and for handling information derived from those activities.

The Note also does not address the role of putative (i.e., commonly accepted or supposed) constraints on domestic security information. Such constraints derive from uncertainty in interpreting regulatory constraints and from concerns about whether domestic security information or its sources might be revealed publicly or to the subjects under investigation. Putative constraints may also result from uncertainty about potential legal liability for impermissible conduct related to domestic intelligence.

Since the completion of the study, significant changes have been made in federal executive orders and departmental guidelines, and in local police department guidelines. For example, on December 4, 1981, after this study was completed, President Reagan issued Executive Order No. 12333 on United States Intelligence Activities, which liberalizes

authority to assist and cooperate with state and local law-enforcement agencies. A recent change at the local level is the abolition of the Los Angeles Police Department's Public Disorder Intelligence Division (PDID), following revelations that copies of police files previously ordered destroyed had been secretly stored at the home of one of the PDID investigators. This is a subject still on the move. The study does not address the regulatory changes or cases prosecuted after 1980.

This Note is a companion to Rand Note N-1901-DOJ, Intelligence Constraints of the 1970s and Domestic Terrorism: Vol. I, Effects on the Incidence, Investigation, and Prosecution of Terrorist Activity, by Sorrel Wildhorn, Brian Michael Jenkins, and Marvin M. Lavin, December 1982. This work was funded by the Law Enforcement Assistance Administration of the Department of Justice.

SUMMARY

Domestic security investigations are primarily concerned with acts of domestic terrorism--that is, with unlawful past, current, or planned acts of politically or socially motivated violence in the United States. These investigations seek "domestic intelligence," information that will lead to the conviction and punishment of the perpetrators of past acts of terrorist violence, ameliorate the consequences of current acts, and forestall the commission of planned acts.

Virtually every aspect of domestic security investigations is constrained by rules, which are continually changing, generally in the direction of increased hindrances. This Note presents a survey of readily available source materials dealing with constraints of the 1970s on the collection, maintenance, use, and dissemination of domestic intelligence. It describes legal, legislative, and administrative constraints that arose or were modified during the 1970s, a decade of particularly marked changes.[1] It does not examine the recent changes made by the Reagan Administration.

We identify five aspects of domestic security investigations: initiation, kinds of information gathered, techniques of information

[1] This study is limited to domestic intelligence; it does not consider constraints on foreign intelligence or foreign counterintelligence, which are also basic sources of information concerning terrorist acts in the United States. It does not assess the effects of Executive Order 12036 (United States Intelligence Activities, January 1978) or the Foreign Counterintelligence Guidelines of the U.S. Department of Justice on domestic security investigations. Thus, issues concerning intelligence pertaining to transnational terrorism--i.e., terrorism involving both U.S. and non-U.S. persons, facilities, and communications--are beyond the scope of this study. This limitation is based, in part, on the unavailability of source materials.

gathering, handling of information, and reporting and controlling of investigations. A gross distinction is made between constraints emanating from legal sources (e.g., constitutions, statutes, judicial decisions) and those imposed by administrative authority. A further distinction is made among federal, state, and local constraints.

INITIATION OF DOMESTIC SECURITY INVESTIGATIONS

The decision to undertake a domestic security investigation is constrained by administrative guidelines that have been developed to aid in determining whether the character and activities of target organizations or individuals justify the initiation of intelligence gathering. A leading issue in formulating these constraints is whether they should be based on a "criminal act" standard or on something less stringent, i.e., should domestic security investigations be initiated only if a law-enforcement agency has first attained a specified level of confidence that a violent crime (or a conspiracy to commit one) has occurred, is in progress, or is imminent, or should a lesser standard prevail?

This survey focuses on the following major regulatory constraints:

- The Attorney General's Guidelines for FBI Domestic Security Investigations (March 10, 1976). These guidelines distinguish among three types of FBI investigations: preliminary, limited, and full. The guidelines do not mandate a strict "criminal" standard for initiating security investigations. Indeed, on August 30, 1976, the FBI itself adopted a more stringent policy concerning the initiation of security investigations.
- The Seattle Police Intelligence Ordinance. This ordinance, enacted by the city of Seattle on January 1, 1980, established

policies to govern the Seattle Police Department on intelligence matters, particularly those relating to intelligence investigations involving "restricted information," i.e., information concerning political or religious associations, activities, beliefs, or opinions.

- o Intelligence guidelines and procedures of the New York City Police Department (NYPD) and the Los Angeles Police Department (LAPD). The Procedures for Public Security Activities of the NYPD Intelligence Division and Proposed Operations Guidelines for the LAPD Public Disorder Intelligence Division prescribe who has the authority to initiate an investigation to obtain intelligence information, by whom the investigation may be conducted, under what conditions, and for what purposes.
- o Case law, statutory law, and executive orders. Legal and administrative constraints have been enacted to provide a basis for determining whether police intelligence-gathering activities are inherently lawful and whether specific law-enforcement agencies have legal authority to initiate security investigations. State and federal jurisdictions have generally upheld the legality of law-enforcement intelligence activities, provided the government "can demonstrate a `compelling' state interest which justifies the resultant deterrents of First Amendment rights and which cannot be served by alternative means less intrusive on fundamental rights."[2] However, the security investigation authority of the FBI has been questioned because it is not clearly spelled out.

---

[2] White v. Davis, 13 Cal.3d 757 (1975).

The major concerns about domestic security investigations involve the standards defining justifiable intelligence gathering. The requirement that criminal activity must be present to justify initiation of an investigation remains contentious, and safeguarding fundamental rights--including privacy and the First Amendment freedoms--is often a frustrating mandate.

CONSTRAINTS ON THE KINDS OF INFORMATION GATHERED

In the 1950s, legal and administrative constraints proliferated, reflecting concern with First Amendment rights and with rights of privacy, as well as continuing attention to Fourth Amendment (search and seizure) rights and others. As a result, approval must be obtained from an objective magistrate for security investigations to gather personal information of various kinds by certain means, and the subjects of the investigations have to be informed that investigations have been initiated.

Direct Investigatory Controls

The investigatory-control instruments considered in this Note set forth the kinds of information that may and may not be gathered in an intelligence investigation. For example, the LAPD guidelines prohibit the recording of information about political or religious activities, beliefs, or opinions of an individual, group, or organization unless such information is relevant to a significant threat to public order. Information on individuals' personal associations may be recorded only if it relates to unlawful public disorder, threats to life and property, or unlawful interference with civil rights.

First Amendment Protections

Although some public meetings are a clear source of concern to those responsible for domestic security, it is widely asserted that police monitoring of such meetings stifles the free expression of ideas and deters free association. An acceptable balance must be reached between these chilling effects on First Amendment rights and the avoidance of public violence and governmental disruption. The courts have consistently held that reasonable intrusions on First Amendment rights are permissible when a compelling state interest is involved.

Privacy Protections

Constitutional rights of privacy have generated a large and diverse body of statutes, court decisions, and administrative regulations, limiting the kinds of information that may be gathered in domestic security investigations.

Seven states have enacted omnibus statutes regulating individually identifiable information held by government agencies, including the disclosure of such information to other government agencies. Four of these statutes apply to local as well as state agencies. They all generally resemble the federal Privacy Act of 1974.

Statutory privacy protections also exist at the state level for specific kinds of government records on individuals, including criminal-justice information, court records, student records, tax records, welfare records, arrest records, mental health service information, juvenile-court records, and alcohol and drug abuse treatment records. All of the omnibus privacy statutes exempt criminal investigative records; all differ in their provisions for disclosure of personal information pursuant to compulsory legal process.

Some types of privately held personal information are also regulated by state statute. These include

- Consumer reporting (i.e., fair credit-reporting and investigation) records (17 states).
- Financial and credit-granting records (16 states).
- Arrest records (26 states).
- Employment records (5 states).
- Medical records (47 states).
- School records (32 states).
- Tax records (30 states).
- Wiretap records (38 states).

Statutory Law

Statutory laws that regulate specific kinds of information commonly involved in security investigations include

- The Privacy Act of 1974, which limits the collection, maintenance, use, and dissemination of personal information by federal agencies.
- Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (as amended in 1970, 1971, 1978), which regulates wiretapping and electronic eavesdropping.
- The Family Educational and Privacy Rights Act, which limits disclosure of personally identifiable information in education records.

- The Tax Reform Act of 1976, which provides for confidentiality of federal tax returns and tax return information.
- The Right to Financial Privacy Act of 1978, which prohibits disclosure of any customer's financial records held by a financial institution to any federal authority except by defined processes.
- The Fair Credit Reporting Act of 1970, which limits the preparation and disclosure of consumer and investigative consumer reports.
- The Foreign Intelligence Surveillance Act of 1978, which provides for handling of information concerning a U.S. person, acquired from electronic surveillance of agents of foreign powers engaged in criminal activities.
- The California Financial Privacy Act of 1976, which restricts disclosure of a customer's financial records held by a financial institution to a state agency (basically equivalent to the federal Right to Financial Privacy Act of 1978).

California Case Law

During the 1970s, California courts ruled on a number of significant cases involving rights to (and the expectation of) privacy concerning personal information. Cases in which violations of rights to privacy were found include

- People v. McKunes, where a government agent obtained records of telephone calls from the telephone company without legal process.

- o Burrows v. Superior Court, where a sheriff and a prosecutor acquired bank statements with the consent of the bank but without legal process.
- o People v. Blair, where the police obtained a list of credit card charges without legal process.
- o Tavernetti v. Superior Court, where a telephone lineman intercepted a conversation about an illegal transaction and reported it to the police.
- o People v. Meija, where the police elicited a record of telephone calls made from a motel room without advance judicial sanction.
- o People v. Krivda, where the police made a warrantless search of trash-barrel contents after pickup by a refuse truck.
- o People v. Arno, where observations were made through an upper-story office window from an adjacent hillside by police using binoculars.

REGULATION OF TECHNIQUES OF INFORMATION GATHERING

Regulation of the techniques of intelligence gathering is a major concern. The Attorney General's Guidelines, the Seattle Police Intelligence Ordinance, and the Procedures for the NYPD Intelligence Division provide explicit constraints on the use of informants, mail covers, electronic surveillance, undercover agents, photo surveillance, and other techniques. They set forth the conditions justifying the use of intelligence-gathering techniques and the procedures to be followed.

FBI Use of Information-GatheringTechniques

The use of information-gathering techniques by the FBI is subject to the following rules:

- o Undercover agents. Use of undercover agents must be authorized by the Special Agent in Charge within each FBI field division, who coordinates with the U.S. Attorney in the jurisdiction. These operations must respect limitations imposed by the First, Fourth, Fifth, and Sixth Amendments to the Constitution, pertinent statutes and executive orders, Department of Justice regulations and guidelines, and internal FBI administrative and operational procedures.
- o Mail covers. Mail covers may be used only in full investigations and with the approval of the Attorney General. They must conform to the regulations set forth in Part 831 of the Postal Manual, as administered by the Chief Postal Inspector.
- o Electronic surveillance. Electronic surveillance may be undertaken only on an order of a U.S. district court, under the provisions of Title III, or with the consent of a party to the communication. Department of Justice booklets contain step-by-step procedures.
- o Physical surveillance. The FBI Manual of Investigative Operations and Guidelines (MIOG) distinguishes between fixed and mobile surveillance and, within these two categories, between close and loose observation. It mandates who can perform the surveillance under what supervision, and it

specifies the surveillance logs that must be maintained; it does not give detailed descriptions of surveillance techniques.

- o Other Techniques. FBI agents have no formal, written, specific procedures for the use of trash covers, the conduct of interviews, or the elicitation of third-party or other-government-agency records.

Electronic Surveillance

Constraints on the use of electronic surveillance for intelligence gathering reflect the continual attention of the U.S. Supreme Court to the issue of what constitutes a "search" under the Fourth Amendment and the reaction of legislatures to the Court's decisions. Landmarks in federal case law, statutory law, and administrative policy affecting the conduct of electronic surveillance are reviewed here, beginning with Olmstead v. United States (1928) (where it was held that physical trespass must be present for illegal interception to have occurred).

The basic federal statute regulating electronic surveillance is Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (and its subsequent amendments of the 1970s). This statute forbids, with certain exceptions, all forms of unauthorized wiretapping and eavesdropping. (The exceptions are reviewed in this Note.) Misuse of electronic surveillance involves significant penalties, and the subjects of the surveillance must be promptly informed of its use, current or proposed.

State laws pertaining to electronic surveillance generally follow federal law closely. California law, however, which allows no wiretap warrants, is more stringent than federal law.

Informants and Undercover Agents

Legal and administrative constraints on the use of informants and undercover agents to obtain domestic intelligence information have emerged slowly and selectively. The courts have consistently held that police undercover activities are lawful when there is a compelling state interest. However, the major instruments of direct investigatory control impose explicit constraints on when, where, how, and against whom undercover agents and informants may be used.

The U.S. Supreme Court has found that law-enforcement agencies have broad discretion in the use of these techniques. It has ruled that

- The Fourth Amendment does not prohibit court testimony about a defendant's statement to an informant, howsoever the informant recorded or transmitted the conversation.
- The Fifth Amendment privilege against self-incrimination is not violated, in the absence of coercive tactics or custodial interrogation, when an informant elicits incriminating verbal information from a suspect.
- A mere invasion of the attorney-client relationship by an informant does not violate the Sixth Amendment right to counsel, regardless of the way in which an intercepted conversation is used in the criminal proceedings. The proceedings must have commenced and the informant's report must relate to the specific charge against the defendant for the informant's presence to be a violation.

- o An informant's activities are not unconstitutional on federal due-process grounds, i.e., as shockingly unfair police practices.
- o The use of informants does not taint federal criminal justice.
- o The protection afforded by the First Amendment against intelligence gathering and, in particular, against informant use is undetermined.

Entrapment

The majority view of a closely divided U.S. Supreme Court continues to be that entrapment (i.e., police conduct that can be a basis for an affirmative legal defense in a criminal proceeding) is proved only if (1) government investigation and inducement overstepped the bounds of permissibility and (2) the defendant did not harbor a preexisting criminal intent. Here, entrapment is for the jury to decide. In contrast to this "subjective" test, the minority view supports an "objective" test of the law-enforcement activity alone, with the defendant's conduct being irrelevant. This is decided by the judge rather than the jury. Some state laws, e.g., California's, adopt an intermediate position concerning entrapment.

CONSTRAINTS ON THE HANDLING OF INTELLIGENCE INFORMATION

The handling of intelligence once it has been gathered is subject to a variety of legislative, judicial, and administrative constraints.

NYPD Intelligence-Handling Procedures

When Public Security police officers of the NYPD obtain intelligence information, they must designate the source of the information; when an informant is the source, they must also provide an evaluation of the informant's reliability. All raw intelligence information must then be evaluated by an analysis section before being reported, recorded, filed, or disseminated. Information deemed to lack substantial relevance to the Public Security mission is destroyed by the chief analyst or the commanding officer of the Intelligence Division. The intelligence that is retained is formally classified as to (1) importance, (2) time priority, (3) source reliability, and (4) content substantiation.

After the information has been evaluated and classified, the need for additional data may be observed. All available data on the subject being investigated are then assembled and analyzed, and the Intelligence Division commander decides whether to accept and report the analysis, to require its revision, or to direct further investigation.

Intelligence that is found to meet specified criteria is recorded on index cards, which indicate the classification and source of the intelligence and are color-coded by year.

Criteria have been established for disseminating Public Security information, distinguishing between intradepartmental and interdepartmental distribution; dissemination to nongovernmental individuals or agencies is forbidden. A special, more restrictive set of criteria and procedures applies to surveillance photos.

Frequent review by specified officials is mandated to determine whether filed information should continue to be collected and retained. And every file card must be reviewed within two years of its initial filing to determine whether it should be kept active, placed in a dormant file for reevaluation within two years, or purged and destroyed.

Freedom-of-Information and Privacy Laws

Freedom-of-information and privacy laws regulate public access to personal information held by law-enforcement agencies and to information about those agencies; access by subject individuals and organizations to personal and organizational information held by law-enforcement agencies; and access by law-enforcement agencies to personal and organizational information held by other government agencies and private organizations.

These laws are a source of significant uncertainty about access to and disclosure of intelligence information, its sources, and the techniques of gathering it. The uncertainties generate considerable litigation and exacerbate the impacts of the laws on government conduct and on domestic security investigations.

The Freedom of Information Act (FOIA), enacted in 1966 and significantly amended in 1974, requires federal agencies to make available all information held by them to any person who requests it, unless the information falls within one of nine narrowly construed exemptions. The FOIA also provides that any reasonably segregable portion of a record shall be provided to the requestor after deletion of portions that are exempt.

The seventh exemption from mandatory disclosure--the one most relevant to law-enforcement (including domestic security) information--places the burden on the law-enforcement agency that denies record disclosure to justify such denial, if the requestor sues in federal district court to compel disclosure.

Federal investigatory files for law-enforcement purposes, which generally include files of federal domestic security investigations, are largely exempted from mandatory disclosure under the FOIA by the seventh exemption. But the courts have tended to rule that denial of disclosure of requested investigatory records is justified only if such disclosure would interfere with ongoing enforcement proceedings.

Nearly every state has a freedom-of-information or open-public-records statute requiring that state government records be available for public inspection. These statutes may provide exemptions, either permissive or mandatory, for specific types of records. Law-enforcement records are customarily given a permissive exemption from disclosure, but the courts tend to construe the exemptions narrowly. Some states have enacted statutes that provide for the confidentiality of specific government-maintained records (e.g., criminal-history information) and override their open-records statutes.

Exempt information held by law-enforcement agencies may be open to discovery in a criminal proceeding if the court finds the information to be essential to a fair trial. The consequence of nondisclosure in these circumstances can be dismissal of criminal charges. Thus, the shield for domestic security intelligence provided by exemption is not necessarily reliable or certain.

The Privacy Act of 1974 is intended to safeguard personal privacy by limiting the collection, maintenance, use, and dissemination of personal information by federal agencies. The Act imposes a variety of requirements on systems of records containing information that can be accessed by personal identifiers. Three types of exemptions are contained in the Act:

- Conditions of disclosure--conditions under which an agency may disclose a personal record without prior written consent of the subject.
- General exemptions--system characteristics that enable an agency head to promulgate rules exempting the system from most of the Act.
- Specific exemptions--system characteristics that enable an agency head to promulgate rules exempting the system from specified requirements of the Act.

Because of the conditions of disclosure, the Privacy Act does not erect effective barriers to the transfer of federal law-enforcement information on individuals among federal and other law-enforcement agencies. It appears that the Congress intended that federal criminal law-enforcement agencies should have broad immunity from the requirements of the Privacy Act, which otherwise might permit access by an individual to investigatory records compiled about him for law-enforcement purposes. However, there is an exemption to the exemptions that provides a legal basis on which the subject of domestic security records could seek to overturn a denial of access. The

interplay of exemptions is another source of uncertainty as to whether domestic security intelligence can be fully and reliably shielded from disclosure.

Interaction of Freedom-of-Information and Privacy Laws

While the Congress intended the FOIA and the Privacy Act to complement each other, they often mesh poorly because of flaws in drafting. Neither act, for example, contains any provision for dealing with the case of an individual requesting his or her records under the FOIA when the holding agency has exempted those records from disclosure under the Privacy Act.

Until case-by-case court decisions and legislative amendments clarify the joint effects of these two laws, the risk that investigatory records might have to be disclosed at some future time cannot be confidently assessed. This uncertainty has been blamed for stifling domestic security investigations by federal law-enforcement agencies. And the uncertainty is probably greatest concerning disclosure of intelligence information that is gathered in an investigation undertaken without a clear expectation of criminal proceedings.

Five of the seven state omnibus privacy or fair-information-practice acts have attempted to anticipate and resolve these conflicts--for example, the Connecticut and Massachusetts privacy acts state that their provisions limiting disclosure do not apply to information whose disclosure is otherwise authorized by statute.

Criminal Proceedings

Domestic security investigations do not necessarily culminate in criminal proceedings, but law-enforcement agencies do generally seek

criminal prosecutions as a result of such investigations, using security investigation information as evidence. However, there are "impediments" to such use in domestic security cases, i.e., factors that limit the utility of security intelligence. These impediments include

- o The exclusionary rule for evidence obtained by an unreasonable search and seizure.
- o Liberal criminal discovery rules, court decisions on criminal discovery that favor the defense, and defense abuses of the discovery process.[3]
- o The defense of discriminatory law enforcement or prosecution.
- o Stringent interpretation of violation of the attorney-client privilege in criminal proceedings.
- o Entrapment tests departing from the subjective standard, i.e., from consideration of the defendant's conduct or predisposition.

REPORTING AND CONTROLLING OF SECURITY INVESTIGATIONS

The Seattle Police Intelligence Ordinance provides an example of an investigatory management device that contains explicit provisions for

---

[3] These include abuses concerning the so-called informant's privilege, i.e., withholding an informant's identity in a criminal proceeding in which his information is sought to be introduced. The U.S. Supreme Court has generally upheld the evidentiary rule of most states that police officers need not, except on matters of the suspect's guilt or innocence, be required to disclose an informant's identity; however, case law varies from state to state.

reporting and control in security investigations. It states that the police may not collect restricted information without an authorization by a commander of a specified rank or higher, and that extensions of the authorization may be given only by the Department Chief and only for additional periods of 90 days. Specific conditions must be met to transmit restricted information to another criminal-justice or governmental agency; the use of infiltrators is prohibited except on written authorization from the Chief; specific instructions must be given to paid informants for carrying out their assignments; and the powers and functions of a criminal intelligence section for processing and analyzing investigative information are strictly defined.

An auditor must be appointed to conduct audits of department files and records, in order to ascertain whether any violations of the intelligence ordinance have occurred; such violations must be investigated by the Chief. Civil liability of the city of Seattle to persons injured by violation of the ordinance is defined, and an annual report on the implementation of the ordinance must be given to city officials and to the public.

CONCLUDING COMMENT

Regulatory constraints on intelligence derived from domestic security investigations grew steadily throughout the 1970s, concurrently with the explosion of information processing technology--and there was a concomitant growth in uncertainty about the scope of those constraints. The effects of this regulatory expansion are considered in companion

Note N-1901-DOJ, Intelligence Constraints of the 1970s and Domestic Terrorism: Vol. I, Effects on the Incidence, Investigation, and Prosecution of Terrorist Activity, by Sorrel Wildhorn, Brian M. Jenkins, and Marvin M. Lavin, December 1982.

CONTENTS

I. INTRODUCTION [1]

During the early 1970s, governmental investigations of antiwar activism and the homicides at Kent State University aroused widespread criticism of the methods and procedures of the Federal Bureau of Investigation (FBI). In 1971, a conference of activist critics and scholars of the FBI, held at Princeton University, concluded that publicly identified improprieties would thereafter undermine public opinion toward the FBI. Later, in June 1972, the U.S. Supreme Court ruled that the umbrella of "national security" could no longer be invoked to justify the use of intrusive techniques by federal investigators in domestic security cases.[2]

Investigative improprieties were also publicly revealed during the Watergate inquiries and the investigation into the possible impeachment of President Nixon. These were followed by the enactment of the Privacy Act of 1974[3] and by allegations in the New York Times, confirmed by the Director of Central Intelligence, of illegal domestic investigations by CIA personnel. In January 1975, the U.S. Senate established a Select Committee on Government Operations with respect to Intelligence Activities, known as the Church Committee. The House of Representatives thereafter also reorganized its own intelligence system.

---

[1] The review of domestic intelligence in this section was contributed by William R. Harris, The Rand Corporation.

[2] The ruling was handed down in the so-called Keith case, which considered electronic surveillance without court order in connection with the bombing of a university research laboratory engaged in classified CIA investigations.

[3] Pub.L. No. 93-579, 5 U.S.C. Sec. 552a (Supp. V, 1975).

Congressional scrutiny of U.S. intelligence activities in 1975-76 encompassed all U.S. intelligence agencies. CIA activities and the counterintelligence activities of the FBI, particularly a program known as COINTELPRO, received widespread public attention at that time.

The Executive branch and the Congressional Committees jointly developed new guidelines for domestic intelligence activities, which President Ford issued in an Executive Order on February 18, 1976.[4] This order, which was substantially reaffirmed by President Carter's Executive Order of January 1978,[5] limited foreign intelligence and counterintelligence investigations of "U.S. persons," including aliens permanently residing in the United States.[6]

After extensive Congressional consultation, Attorney General Levi issued new Guidelines for FBI Domestic Security Investigations on March 10, 1976. On August 30, 1976, the FBI itself adopted a more stringent policy restricting domestic security investigations of individuals based upon organizational affiliations.

In the aftermath of these federal reforms, various municipalities adopted regulatory safeguards for domestic intelligence collection and use. The Los Angeles Police Department adopted new standards and procedures in December 1976; Seattle enacted a police intelligence ordinance in 1979; and several states established guidelines for safeguarding "criminal history record information" held by law-enforcement agencies.

---

[4] United States Foreign Intelligence Activities, Executive Order No. 11905, February 18, 1976, 41 F.R. 7703.

[5] United States Intelligence Activities, Executive Order No. 12036, January 24, 1978, 43 F.R. 3674.

[6] See E.O. No. 12036 for the current definition of "U.S. person."

Transition teams of the incoming Reagan Administration considered reforming the system that regulates intelligence on terrorism, and an interagency working group chaired by the General Counsel of the CIA reportedly proposed revisions of Carter's Executive Order concerning U.S. intelligence activities. Most recently, the Heritage Foundation has recommended regulatory reforms that would lower the threshold for federal investigations of both domestic and international terrorism.

This Note presents a survey of the major regulatory constraints on the collection, maintenance, use, and dissemination of domestic intelligence information pertaining to acts of terrorism in the United States in the 1970s. We consider two broad categories of constraints: legal, which stem from constitutional, legislative, and judicial sources; and administrative, typically agency guidelines, orders, rules, prohibitions, etc., that implement policy and/or interpret legal constraints in the context of an agency's operations. These constraints apply to the following aspects of domestic security activities:

- Initiation of security investigations[7]
- Kinds of information gathered
- Techniques of information gathering
- Information handling (including criminal proceedings)
- Reporting and controlling of security investigations

---

[7] The term security investigation denotes a domestic security investigation, including the investigation of criminal acts that are politically motivated, as distinguished from a more or less exclusively criminal investigation and from a more or less exclusively foreign intelligence or counterintelligence investigation. This usage does not necessarily coincide precisely with that of particular law-enforcement agencies.

These five aspects are considered separately in the following sections of this report.

II. INITIATION OF DOMESTIC SECURITY INVESTIGATIONS

OVERVIEW

Revelations about past abuses in domestic security investigations have led to the formation of rules for determining whether the character and activities of target organizations and individuals justify the initiation of such investigations.[1] These constraints appear in

- Relevant parts of the Attorney General's Guidelines, which are likely to be legislated in some form within the pending FBI charter.
- A local ordinance establishing policies governing the initiation of security investigations by the Seattle Police Department.
- Proposed operational guidelines (April 22, 1980) for the Los Angeles Police Department's Public Disorder Intelligence Division (PDID), developed jointly by the Board of Police Commissioners and the Police Department for the initiation, conduct, and reporting of intelligence investigations.

---

[1] Congressional hearings, particularly in connection with proposed FBI charter legislation, have, in fact, addressed the question of whether (federal) security investigations should be barred altogether. The position of the ACLU on the elimination of the FBI security investigation role was voiced in hearings before the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary, House of Representatives, 94th Congress, Part 3, 1975-76, dealing with FBI oversight. The question is also argued in detail in J. Berman, "FBI Charter Legislation: The Case for Prohibiting Domestic Intelligence Operations," University of Detroit Journal of Urban Law, Vol. 55:853, 1978.

- o Current (initially effective circa 1972) guidelines within the New York City Police Department entitled Procedures--Public Security Activities of the Intelligence Division, which regulate the initiation of intelligence investigations and the procedures and methods to be used for gathering, evaluation, analysis, reporting, recording and storage, and dissemination of intelligence information.
- o Various statutes and decisions pertaining to the legality of conducting security investigations.

The central issue in establishing criteria for activating security investigations is whether to use a criminal standard or a less stringent standard. That is, should an investigation be permitted only if the law-enforcement agency involved has determined, with a specified level of confidence, that a violent crime (or conspiracy to commit one) has occurred, is in progress, or is imminent?

CONSTRAINTS ON THE INITIATION OF INVESTIGATIONS

The Attorney General's Guidelines[2]

The Attorney General's Guidelines set out bases for the initiation of FBI domestic security investigations as follows:

> Domestic security investigations are conducted ... to ascertain information on the activities of individuals, or the activities of groups, which involve or will involve the use of force or violence and which involve or will involve the violation of federal law, for the purpose of:

---

[2] The Attorney General's Guidelines are reproduced in Appendix A. See also John T. Elliff, The Reform of FBI Intelligence Operations, Princeton University Press, Princeton, New Jersey, 1979; and the GAO statement before the Subcommittee on Civil and Constitutional Rights in Hearings on FBI Charter Proposals, November 9, 1977 (the follow-up report on FBI domestic intelligence operations).

1. overthrowing the government of the United States or the government of a State;

2. substantially interfering, in the United States, with the activities of a foreign government or its authorized representatives;

3. substantially impairing for the purposes of influencing U.S. government policies or decisions:

   (a) the functioning of the government of the United States;
   (b) the functioning of the government of a State; or
   (c) interstate commerce

4. depriving people of their civil rights under the Constitution, laws, or treaties of the United States.

The Guidelines distinguish among three types of domestic security investigations: preliminary, limited, and full.

Preliminary investigations may be initiated by FBI field officers on their own judgment, given allegations or other information that an individual or a group may be engaged in activities that involve or will involve the use of force or violence and the violation of federal law for one or more of the purposes enumerated above. A preliminary investigation determines whether or not there is a factual basis for initiating a full investigation. It permits physical surveillance and interviews only for the limited purpose of identifying the subject of an investigation.

Limited investigations, which must be authorized by a Special Agent in Charge or by FBI Headquarters, are opened when preliminary investigations prove inadequate to determine whether there is a factual basis for full investigations. A limited investigation permits physical surveillance and interviews for purposes other than identifying the subject of the identification.

Full investigations, which must be authorized by FBI Headquarters, may be initiated only on the basis of specific and articulable facts that give reason to believe that an individual or a group is or may be engaged in activities as described under preliminary investigations. Authorization depends on four factors:

1. The magnitude of the threatened harm.
2. The likelihood that it will occur.
3. The immediacy of the threat.
4. The danger to privacy and free expression posed by a full investigation.

Clearly, the Guidelines do not mandate a strict "criminal" standard for initiating a security investigation--that is, they do not insist on probable cause to believe that a crime has been or is being committed; on the other hand, they do not allow even a preliminary investigation on the basis merely of speech or association that prompts law-enforcement concerns.

The Guidelines are stated in FBI manuals that govern investigators.[3] In addition, the FBI adopted a more stringent policy on security investigations on August 30, 1976:

> When the basis for investigation of an individual is affiliation with an organization, the investigation may be initiated only where such organization is the subject of a full investigation. Membership or affiliation alone is not an adequate basis for investigation. It must be shown that the individual is in a policymaking position in the organization or has engaged in activities which indicate he is likely to

[3] We were not given access to the relevant sections of FBI manuals, so we do not know how the Guidelines are presented and interpreted therein.

> use force or violence in violation of a Federal law. In addition, the investigation should focus on these activities done in active support of the organization and separate violations of law involving the individual.[4]

Thus, preliminary investigations are begun by the FBI only when information is received that a person is a leader of or has engaged in activities that would make him or her subject to full investigation. Names of organization members not meeting the criteria for investigation are indexed for future reference.

The Guidelines permit the FBI wide discretion to initiate and conduct preliminary investigations at the local level, but full investigations must not only be authorized by FBI Headquarters, they are monitored and reviewed by the Attorney General. An Investigations Review Unit (IRU) was created soon after the adoption of the Guidelines to review FBI justifications for initiating full investigations and to recommend approval or disapproval by the Attorney General. The IRU evaluations have consistently recommended full investigation only in cases of activities that made violence a credible threat in the foreseeable future.[5] During the first year in which the Guidelines were in effect, there was some confusion about when preliminary investigations should be initiated on individuals as a by-product of full investigations of other individuals or of organizations.[6]

---

[4] Quoted in the GAO follow-up report, op. cit.
[5] Ibid., p. 20.
[6] Ibid., pp. 28-30.

The Seattle Police Intelligence Ordinance

On July 2, 1979, the Seattle City Council enacted Ordinance #108333 (effective 1 January 1980) establishing

> ... policies governing the Seattle Police Department in collecting, receiving, and transmitting information; establishing procedures, controls, and prohibitions on the collection and use of particular types of information; regulating and forbidding certain police operations; establishing the powers of a criminal intelligence section and its personnel; and providing enforcement procedures, administrative penalties, and civil remedies.

This pathbreaking local legislation provides for

> ... the collection and recording of information for law enforcement purposes, so long as these police activities do not unreasonably: (a) infringe upon individual rights, liberties, and freedoms guaranteed by the Constitution of the United States or of the State of Washington--including, among others, the freedom of speech, press, association, and assembly; liberty of conscience; the exercise of religion; and the right to petition government for redress of grievances; or (b) violate an individual's right to privacy.

This law focuses especially on restricted information, i.e., information pertaining to

> (i) an individual's political or religious associations, activities, beliefs, or opinions;
>
> (ii) the political or religious activities, beliefs, or opinions and the membership, mailing, subscription, or contributor lists of a political or religious organization, an organization formed for the protection or advancement of civil rights or civil liberties; or
>
> (iii) an individual's membership or participation in such an organization, in a political or religious demonstration, or in a demonstration for community purposes.

Restricted information may not be collected unless the subject of the information is reasonably suspected of criminal activity or the information relates to the reliability of a victim or witness. The investigation must be authorized by a lieutenant or higher-ranking police officer. The authorization may be a written request from a prosecuting attorney, a city attorney, or the Attorney General of Washington or of the United States. Under emergency conditions, restricted information may be collected without authorization, but it must be purged within 24 hours if an authorization is not granted.

When there is reasonable suspicion that the subject of restricted information could pose a threat to the life or safety of a visiting official or dignitary, the Chief of Police may authorize an investigation. In these cases, the responsible police personnel need no authorization for collecting restricted information from public records, from any person who is planning a demonstration or activity in connection with the visit (the planner must be advised of the purpose of the inquiry), from another government agency (the availability of information, however, depends upon the agency's sources), or from unsolicited sources.

Other aspects of the Seattle ordinance will be considered later in this Note as they relate to other domestic security activities.

Proposed Operational Guidelines for the Los Angeles PDID

On April 22, 1980, the Los Angeles City Board of Police Commissioners published a set of operational guidelines and reporting procedures for the PDID.[7] These guidelines cover the mission of the PDID, the responsibilities of the PDID and of its commanding officer, and the collection and analysis of intelligence information. Separate guidelines cover the preparation and handling of intelligence reports, briefing reports, rumor reports, and liaison/contact reports and also deal with records of inquiry and of dissemination. Standards and procedures for handling intelligence information files were adopted in December 1976.

The proposed PDID guidelines permit the initiation of preliminary investigations on the basis of information that an organization or individual may be engaged in activities having a potential for violence, property damage, or disorder; deliberate and concerted illegal behavior as a form of protest; past, current, or pending criminal acts that would be disruptive of public order; or terrorism. These investigations are initially confined to determining whether a reasonable basis exists for an in-depth investigation. Initiation of an in-depth ongoing investigation requires the approval of the Commanding Officer of the PDID. The Chief of Police, the Director of the Office of Special

[7] These guidelines are an interim product of a program conducted by the Police Commission and the Police Department, beginning in 1973, to address the collection and management of intelligence information. The retention and maintenance of intelligence files were the main concern of the PDID Standards and Procedures, publicly reported in April 1975 and adopted in December 1976. The proposed guidelines are primarily concerned with the gathering and collection of intelligence and with intelligence reports. Future guidelines are expected to concentrate on proper dissemination of intelligence information.

Services, the Commanding Officer of the PDID, or the Officer in Charge of a PDID section may direct the initiation of an investigation concerning an event, situation, person, group, or organization, but he must specify the purpose or objective of the investigation. Ongoing investigations must be approved by the Commanding Officer of the PDID. Finally, only individuals and organizations on whom files are maintained in compliance with existing PDID guidelines may be targeted for surveillance.

Procedures for Public Security Activities of the NYPD

In New York City, only the Police Commissioner, the First Deputy Commissioner, the Chief of Inspectional Services, and the Commanding Officer, Intelligence Division, have authority to initiate an investigation to obtain intelligence information about events or situations that

- Have the potential for violence or disorder.
- Adversely affect the availability of foods and services to the public.
- Create traffic, crowd-control, or noise problems.
- Require notification to, or coordination with, other city, state, or federal agencies.
- Would have serious national and/or international ramifications if violence or disorder should ensue.
- Involve deliberate and concerted illegal behavior as a form of protest.
- Foment intergroup hostilities, counterdemonstrations, assaults, destruction of property, etc.

- o Involve groups or individuals advocating (1) violence and/or violent attacks on government operations or on police officers or other public officials, (2) racial, religious, or ethnic conflict between religious and ethnic groups, or (3) achievement of goals by unlawful means.

The purpose of an investigation must be specified by the official who directs its initiation. The Commanding Officer of the Intelligence Division, subject to the review of the Police Commissioner or his First Deputy, is responsible for initiating additional investigation when the information obtained by a public security investigation shows that further investigation is warranted.

Other Legal Constraints

A California court case in 1975 raised the issue of whether the Los Angeles Police Department could lawfully conduct a covert intelligence gathering activity with undercover officers as registered students at state universities.[8] A taxpayers' suit sought an injunction to prohibit use of public funds for an undercover operation at UCLA, alleging that the police agents involved compiled and submitted secret reports that pertained to no illegal activity. The trial judge sustained a demurrer to the complaint, but the California Supreme Court reversed the decision and remanded the controversy for trial.

---

[8] White v. Davis, 13 Cal.3d 757 (1975). We shall frequently use California law for substantive illustrations partly because of its often-innovative nature and partly because of our relative familiarity with it. California law may, however, not be representative of that in other states.

The Supreme Court held that "In view of ... [the] significant potential chilling effect, ... surveillance activities can only be sustained if defendant can demonstrate a 'compelling' state interest which justifies the resultant deterrents of First Amendment rights and which cannot be served by alternative means less intrusive on fundamental rights." The Court ruled that the alleged police surveillance and data-gathering activities constituted a prima facie violation of the State Constitution's guarantee of the right of privacy. It declared that while the latter "... does not purport to invalidate all such information-gathering, it does require that the government establish a compelling justification for such conduct." In concluding that the lawsuit did state a cause of legal action, the Court expressed a fundamental constraint on the power of law-enforcement agencies to initiate and conduct security investigations.

The broader question of whether or not police intelligence gathering activities, i.e., security investigations, are inherently lawful has been addressed in a number of court cases in which the legality of such activities has been upheld.[9] In Anderson v. Sills,[10] the New Jersey Supreme Court reversed a lower court summary judgment against groups seeking in a class action to restrain the implementation of a statewide intelligence arrangement and remanded for a trial on the merits. The intelligence arrangement was created in the

---

[9] The Erosion of Law Enforcement Intelligence and Its Impact on the Public Security, Report of the Subcommittee on Criminal Laws and Procedures to the Committee of the Judiciary, 95th Congress, 2nd Session, GPO, Washington, 1978. See Chap. V, "Is Law Enforcement Intelligence Legal? A Summary of Court Rulings," pp. 43-48.

[10] 56 N.J. 210 (1970).

aftermath of destructive riots in Newark in 1967. A conference of mayors of New Jersey cities was convened under the aegis of the Governor to consider measures for dealing with such events in the future. The conference prompted an Attorney General's memorandum to local law-enforcement units, soliciting cooperation in sharing intelligence to help prevent and control public disorders. The New Jersey Supreme Court decided unanimously that if there is no intent to control the content of speech, an overriding public need may be met, even though the measure adopted to that end operates incidentally to limit the unfettered exercise of First Amendment rights. The Court declared:

> The police function is pervasive. It is not limited to the detection of past criminal events. Of at least equal importance is the responsibility to prevent crime. In the current scene, the preventive role requires an awareness of group tensions and preparations to head off disasters as well as to deal with them if they appear. To that end the police must know what forces exist; what groups or organizations could be enmeshed in public disorders.[11]

In the case of Socialist Workers Party v. Attorney General,[12] the SWP sought to enjoin the FBI from surveillance of its youth organization, the Young Socialist Alliance, at a convention in St. Louis, Missouri, in December 1974. The suit alleged that these FBI domestic security activities would chill First Amendment rights. A Federal district court granted the injunction, but the Second Circuit Court of Appeals reversed, quoting from United States v. District Court,[13] the so-called Keith case, as follows: "Unless Government

---

[11] As quoted in The Erosion of Law Enforcement Intelligence ..., op. cit., p. 44.

[12] 95 S.Ct. 425 (1974).

[13] 407 U.S. 297 (1972).

safeguards its own capacity to function and to preserve the security of its people, society itself could become so disordered that all rights and liberties would be endangered" (p. 312). The Circuit Court stated: "The FBI has a right, indeed a duty, to keep itself informed with respect to the possible commission of crimes; it is not obliged to wear blinders until it may be too late for prevention." On appeal by the SWP, Justice Marshall, sitting as a circuit justice, upheld the Circuit Court: He found that the SWP had not made a compelling case on the merits in view of the limited nature of the monitoring, the legality of the proposed governmental conduct, and potential injury to the FBI's continuing investigative efforts if the requested injunctions were granted. Justice Marshall stated: "It is true that governmental surveillance and infiltration cannot in any context be taken lightly. The dangers inherent in undercover investigation are even more pronounced when the investigated activity threatens to dampen the exercise of First Amendment rights .... But our abhorrence for abuses of governmental investigative authorities cannot be permitted to lead to an indiscriminate willingness to enjoin undercover investigation of any nature, whenever a countervailing First Amendment claim is raised."

In Fifth Avenue Peace Parade Committee v. L. Patrick Gray,[14] a class action suit against the FBI, the Peace Parade Committee alleged that the FBI's investigation of the Committee's participation in the 1969 mass demonstration against the Vietnam War in Washington, D.C., invaded their right of privacy, chilled their First Amendment rights, and constituted unlawful search and seizure. The remedy requested was

[14] 480 F.2d 326 (1973).

the surrender or destruction of information gathered by the FBI. The Second Circuit Court of Appeals rejected the claim, holding that the FBI acted within its legitimate interests and responsibilities in conducting this security investigation.

Even if police intelligence-gathering activities are not on their face unconstitutional, there remains a question of whether a specific law-enforcement agency has legal authority to initiate security investigations. This issue has been raised primarily in challenges to the FBI's authority for domestic intelligence operations. A legal brief on this authority appeared in the report of the 1976 FBI Oversight Hearings[15] and was included in the GAO report on FBI domestic intelligence operations, as well as in the report of the hearings.[16]

The security investigation authority of the FBI resides in Presidential Directives, in Executive Orders, and in parallel and preexisting statutory provisions. Five Presidential Directives bearing on the FBI's domestic intelligence operations were issued between June 1936 and December 1953. The GAO disagreed with the FBI's reliance on these directives for authority, stating that these "... directives did not, whether considered individually or collectively, explicitly delegate authority to the Bureau to conduct intelligence investigations of subversive activities. To the extent, if any, that they fixed responsibility on the Bureau for such investigations, they did not

---

[15] FBI Oversight Hearings--1976, House of Representatives Subcommittee on Civil and Constitutional Rights, 94th Congress, 1st and 2nd Sessions, September 24, 1975, and February 24, 1976. The brief is reproduced in Appendix D.

[16] FBI Domestic Intelligence Operations--Their Purpose and Scope: Issues That Need to be Resolved, Report to the House Committee on the Judiciary by the Comptroller General of the United States, February 24, 1976, reproduced as an appendix to the 1976 FBI oversight hearings, ibid.

explicitly indicate that all types of domestic groups and individuals were subject to investigation or clearly indicate what constitutes 'subversive activities' or 'subversion.'"[17]

The FBI has interpreted Executive Orders 10450 and 11605, dated April 27, 1953, and July 2, 1971, respectively, as giving the Attorney General responsibility to provide to departments and agencies or the Subversive Activities Control Board information about groups or organizations which could be obtained only through FBI intelligence operations. The statutory authority upon which the FBI primarily relies for its security investigation activities is 28 U.S.C. Sec. 533, whose provisions include the following:

> The Attorney General may appoint officials--
>
> (1) to detect and prosecute crimes against the United States; and
>
> (3) to conduct such other investigations regarding official matters under the control of the Department of State as may be directed by the Attorney General.

The GAO concluded that:

> As to the authority now asserted to conduct domestic intelligence investigations based on 28 U.S.C. 533 and various Executive orders, however, we cannot say that it does not exist. The problem with the FBI's authority even under these delegations remains: it is not clearly spelled out, but must be distilled through an interpretive process that leaves it vulnerable to continuous questioning and debate.[18]

Presumably, the FBI charter now under consideration by the Congress will resolve legal uncertainties about authority for initiating security investigations.

---

[17] Appendix D; also Appendix, p. 167, of the oversight hearings report, op. cit.

[18] Oversight hearings report, op. cit., Appendix, pp. 169-170.

III. KINDS OF INFORMATION GATHERED

The kinds of information gathered in security investigations should be limited to that which is relevant, necessary, and timely, and which does not violate legal protections such as the right to privacy and the First Amendment freedoms.[1] This section discusses these limitations as they are defined in the Attorney General's Guidelines, the Seattle Police Intelligence Ordinance, the proposed operational guidelines for the Los Angeles PDID, and the procedures for the Public Security Activities of the NYPD.

CONSTRAINTS ON INFORMATION THAT CAN BE OBTAINED

The Attorney General's Guidelines

The Guidelines specify that information gathered during preliminary investigations should be pertinent to verifying or refuting the allegations or information that determine whether a factual basis exists for initiating a full investigation of individuals or groups. The information may exist in FBI indexes and files; public records; or federal, state, and local records; it may be derived from previously established informants; or it may be obtained by physical surveillance and interviews for the limited purpose of identifying the subject of an investigation. In a limited investigation, information may be gathered by physical surveillance or interviews for purposes other than that of identifying the subject of the investigation, but that information must

[1] These terms are meaningful, of course, only in relation to the purposes of an investigation. Some purposes, such as the FBI's expressed need to remain informed about the strength, danger, and activities of extremist groups, in addition to pursuing specific criminal investigations, are currently in dispute.

be relevant to the determination of whether there is a factual basis for a full investigation. The kinds of information that may be gathered in a full investigation must relate to the activities of individuals or groups that meet the Attorney General's criteria. The Guidelines do, however, contain provisions for handling certain other information (e.g., information on serious crimes) that is obtained incidentally in the course of a security investigation.

The Seattle Police Intelligence Ordinance

The Seattle ordinance on police intelligence gathering is concerned with two kinds of information, restricted information and private sexual information. It deals with each kind both generally and within the context of administrative records, incidental references, confidential communications, materials open to public inspection, special investigations, and exclusions. The ordinance limits the kinds of information that may be obtained on the basis of relevance to a lawful purpose of the information gathering, the necessity and timeliness of the information, and protection of privacy and First Amendment rights, among others.

Proposed Operational Guidelines for the Los Angeles PDID

The proposed PDID guidelines categorize the kinds of information that may be gathered in terms of sources: overt or covert. Overt sources include PDID personnel, LAPD records, government records, public records, mass media, and special publications. Covert sources are individuals who provide information in confidence and whose identity must remain confidential for their safety. Only information that can be properly maintained in a file, subject to periodic review and audit, may

be recorded. No information may be recorded about the political or religious activities, beliefs, or opinions of an individual, a group, or an organization unless that information is relevant to a significant threat to public order--that is, unless there is a substantial probability of deaths, serious bodily injury, serious property damage, or serious disruptions of vital governmental functions. In general, no information may be recorded about an individual's sexual activities. Recording of information on an individual's personal associations is permitted only if that information directly pertains to the PDID mission.

Procedures for Public Security Activities of the NYPD

The administrative constraints of the NYPD Intelligence Division also categorize information in terms of overt and covert sources. Covert sources are undercover agents (police personnel), informants, court-authorized electronic surveillance, and physical surveillance, including photographic surveillance. Overt sources are NYPD personnel, personnel from other law-enforcement agencies or from non-law-enforcement government agencies, the general public, NYPD records, public records and documents, mass media, publications of various groups, public libraries, and conferences. Public security personnel may gather only information that will, with substantial probability, aid the NYPD to maintain public order, protect life and property, and insure orderly functioning of the city. Information on political beliefs or preferences of any individual, group, or organization is not acceptable as intelligence information unless it concerns public security functions. A similar limitation applies to information on the public habits, predilections, and associates of any

person, either as an individual or as a member of an organization. Restrictions on the kinds of information that may be gathered by electronic surveillance, photographic surveillance, and undercover agents are discussed below.

First Amendment Considerations

The First Amendment guarantees freedom of assembly, speech, redress of grievances, and sometimes religion. However, some public meetings prompt concerns in those responsible for domestic security, and law-enforcement personnel attend these meetings for the stated purposes of

- Obtaining knowledge of current community events and causes.
- Forestalling or restraining riotous conduct.
- Gathering evidence about criminal conduct during public disruptions.
- Identifying individuals and groups with propensities toward future violence.

This presence may stifle the free expression of ideas and may deter free association. It has generally been left to the courts to determine the degree of these chilling effects and the balance between them and avoidance of public violence and governmental disruption. The results of most of the cases involving First Amendment constraints (e.g., White v. Davis) appear to be a reiteration of older court rulings, namely, reasonable intrusions on First Amendment rights are permissible when there is a compelling state interest.

The ability of the courts to draw the fine line between legitimate information gathering and illegitimate investigation of advocacy and association has been questioned on the grounds that domestic security

investigations by definition require surveillance of lawful political activity. Strict statutory procedures governing investigations that may intrude on First Amendment rights have been proposed, some of which go so far as to call for elimination of security investigations, at least by the FBI.[2]

In any event, First Amendment considerations impose constraints on the kinds of information that may be gathered in a security investigation, even though it is difficult to express these constraints as formal rules.

PRIVACY CONSTRAINTS

Constitutional rights of privacy also constrain the kinds of intelligence information that may be gathered in a security investigation. In the following, we indicate the kinds of information

---

[2] The ACLU position has been articulated by J. Berman (FBI Charter Legislation, op. cit., pp. 1050-1051): "If the objective is to permit the FBI to prevent politically motivated criminal acts before they occur, intelligence investigations, by definition, must be initiated without reasonable suspicion that a criminal act has been, or is about to be committed. FBI agents will inevitably focus investigative attention on persons who vigorously dissent against government policy or social conditions, or groups who advocate the need for radical or revolutionary change, even though these activities are constitutionally protected. Dissenters are visible and reasonable targets of intelligence investigations designed to prevent politically motivated violence. Moreover, if the investigative purpose is to piece together a 'web of intelligence,' which intelligence agents claim is required to distinguish real threats of potential violence from 'legitimate conduct,' investigators will have to gather information about the plans, activities, beliefs, associations, and memberships of suspect individuals and groups. The danger is particularly acute when the principal investigative technique involves the use of the planted informer who cannot be entrusted with the decision as to what information about political activity may indicate future violence. The inevitable result of this approach is the very evil which the guidelines and charters are intended to prevent--ongoing investigations of lawful political activity in violation of free speech and associational privacy, unreasonable searches and seizures, and a concomitant 'chilling effect' on all political activity among citizens who are fearful of investigation, exposure, and reprisal if they engage in unpopular political activity."

that are covered by statutes, decisions, and rules that in some way employ privacy considerations. We begin with an overview based on two broad references on privacy law--constitutional, statutory, and judicial: Privacy Law in the States [3] and Compilation of State and Federal Privacy Laws.[4]

Overview

According to Privacy Law in the States, seven states[5] have enacted omnibus statutes regulating all kinds of individually identifiable personal information held by government agencies. These omnibus statutes generally resemble the Federal Privacy Act of 1974 and in four instances apply to local as well as state agencies. Statutory privacy protections also exist for individual kinds of government records on individuals.[6] All seven omnibus statutes exempt criminal investigative records from their provisions, and some grant other exemptions as well, e.g., the California and Arkansas statutes exempt medical-record information. All the statutes regulate the disclosure of personal information to other government agencies.

---

[3] Appendix 1 of Report of the Privacy Protection Study Commission, Government Printing Office, Washington, D.C., July 1977.

[4] R. E. Smith, in Privacy Journal, Washington, D.C., 1978.

[5] Arkansas, Connecticut, Massachusetts, Minnesota, Ohio, Utah, and Virginia.

[6] For example, in California the kinds of data specifically governed by statute include criminal justice information, court records, student records, tax records, welfare records, mental patient records, Insurance Commissioner's records; in Delaware: driving records, public assistance records, adoption records, school records, arrest records, juvenile court records; in Michigan: tax records, drug abuse treatment records, alcohol treatment records, mental health service information, welfare records, bank department records.

The Massachusetts statute requires procedures to assure that an individual is given the opportunity to quash a subpoena for records about himself, and the Ohio law requires that a reasonable effort be made to notify an individual whose personal information is disclosed pursuant to a subpoena. Connecticut requires no notification, and the other four omnibus acts are silent on the issue of the compulsory judicial or administrative legal process. All except Virginia provide for recovery of civil damages in cases of violation of the omnibus privacy act; four impose criminal penalties for certain violations.

The states regulate by statute the following kinds of privately held personal information:

- o Consumer reporting (fair credit reporting). Eleven states have enacted statutes that augment the requirements of the 1970 Federal Fair Credit Reporting Act, which limits the disclosure of certain kinds of information by these private agencies.
- o Financial and credit-granting information. Sixteen states have statutes that specifically address the disclosure of information that banks and other financial institutions maintain about individuals. Alaska, Illinois, Maryland, and California have enacted legislation specifying conditions under which bank records may be disclosed pursuant to compulsory legal process. With some exceptions, disclosure under these laws requires service of process on or notice to the subject of the records. Only Maryland and Louisiana have statutes that prescribe conditions under which a creditor may respond to a subpoena for credit records (as contrasted with general bank

records). Both statutes require that notice of disclosure be given to the debtor.

- o Employment information. Only a few states have laws pertaining to the disclosure of employment information by private-sector organizations.
- o Medical records. Many states have statutes requiring that patient records in public or private hospitals be kept confidential. Physicians are statutorily accorded a confidentiality privilege as to patient information in the majority of states. However, only Michigan provides criminal sanctions for the dissemination of medical-record information without the patient's consent.

Finally, the unprivileged disclosure of any kind of personal information may give rise to a lawsuit alleging invasion of privacy under the common or the statutory law of torts, or similarly might produce a tort suit alleging defamation.

The following overview of the extent of federal and state privacy laws is derived from the Compilation of Federal Privacy Laws:

- o Arrest records. Statutes affecting the availability of arrest information have been enacted in 26 states.
- o Bank records. Nine states have laws that pertain to bank record privacy; three have significant case law in this area. Also, the Federal Tax Reform Act provides that the subject of bank records be given notice of and the right to oppose an administrative summons by the IRS to obtain his bank records.

- o Credit reporting and investigation records. Seventeen states have statutes controlling consumer reporting and consumer credit reporting agencies, particularly disclosure of personal information. Some state statutes resemble the Federal Fair Credit Reporting Act.
- o Employment records. Five states regulate some aspects of employment records in the private sector by statute, but limitation of access does not generally appear to be regulated.
- o Medical records. Privacy of medical information, including the doctor-patient privilege, is covered by legislation in all but three states.
- o School records. The confidentiality of school records is protected by statute in 32 states. A federal law, the Family Educational Rights and Privacy Act of 1974, also regulates access to school records as a condition of receiving federal funds.
- o Tax records. Disclosure of tax information is governed by statute in 30 states. The Federal Tax Reform Act of 1976 requires tax returns and tax return information to be confidential, with specified exceptions (for example, information may be disclosed to federal investigators in non-tax cases if they possess a court order).
- o Wiretap records. Thirty-eight states and the federal government have statutory laws affecting information derived from wiretaps.

Laws Regulating Personal Information

The Federal Privacy Act of 1974.[7] The Federal Privacy Act limits the collection, maintenance, use, and dissemination of personal information by federal agencies. The Privacy Act's restrictions apply only to the federal government and cover all executive departments, the military, independent regulatory agencies, government corporations, and government-controlled corporations; they do not apply to the Congress, the federal courts, the District of Columbia, or the governments of U.S. territories or possessions.

All federal agency record-keeping operations that fit the Privacy Act's definition of a system of records[8] are subject to some of its requirements; however, its scope of application is significantly narrowed by the opportunity it gives some agencies to exempt whole systems from many of its more important requirements.

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (as amended in 1970, 1971, 1978).[9] This Act includes the first

---

[7] Pub.L. No. 93-579, 88 Stat. 1896 (1974), 5 U.S.C. Sec. 552 (Supp. V, 1975).

[8] "The Privacy Act of 1974: An Assessment," Appendix 4 to Report of the Privacy Protection Study Commission, July 1977, p. 7. The following definitions are included in the Act:

"(4) the term 'record' means any item, collection, or grouping of information about an individual that is maintained by an agency including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph;

(5) the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual;"

[9] 18 U.S.C. Sec. 2511 et seq.

federal law specifically regulating the kinds of intelligence information obtained by wiretapping and electronic eavesdropping. Interceptions or oral or wire communications are prohibited, with certain exceptions, e.g., interception with the consent of a party to the communication or interception properly authorized by a federal court.[10] The use or disclosure of information obtained by an unlawful interception is prohibited, and criminal and civil sanctions are provided for violations.

State law may be more stringent than federal law in the protection of communication privacy rights. For example, in California, all parties to the communication must give their consent in order for an interception to be lawful and the information obtained disclosable.[11] By contrast, the federal consent doctrine requires only single-party consent.

The Family Educational and Privacy Rights Act.[12] This Act constrains disclosure of personally identifiable information in education records. Disclosure of such information without parent (or adult student) consent or without legal process of which the parents (or adult student) are given advance notice can result in denial of Federal funding to the school (see subsection (b)(2) of the Act).

---

[10] The Act provides also that when a State statute so authorizes, a competent State court may authorize electronic surveillance when the interception may furnish evidence of one of a broad set of specified crimes.

[11] See California Penal Code Secs. 631 and 632, which cover wiretapping and eavesdropping, respectively.

[12] 20 U.S.C. Sec. 1232g.

The Tax Reform Act of 1976.[13] This federal legislation provides that tax returns and tax return information are confidential and subject to disclosure only as permitted by Sec. 6103 of the Act. Disclosure may be made to a designee of the taxpayer or to a person (such as a spouse) who has material interest; to a state tax official to administer state tax laws if there is a state law protecting the confidentiality of the information; and, for specified purposes, to Congressional committees, the White House, the Treasury Department and Justice Department in civil and criminal tax cases, federal agencies in non-tax criminal cases (upon grant of an ex parte order by a federal judge), and the General Accounting Office. Unauthorized disclosure is a felony, and civil remedies are also available.

Right to Financial Privacy Act of 1978.[14] This law prohibits disclosure of personal financial information held by a financial institution to any federal government authority except pursuant to an authorized administrative subpoena or summons, search warrant, judicial subpoena, or formal written request.[15] The subject of the records must be given notice and an opportunity to oppose the disclosure. However, the notice may be delayed by an order of an appropriate court if the government authority shows that the records being sought are relevant to a legitimate law-enforcement inquiry and that the notice would likely result in flight from prosecution, intimidation of witnesses, endangering life, destruction of evidence, etc.

---

[13] 26 U.S.C. Sec. 1 et seq.

[14] 12 U.S.C. Sec. 3401 et seq.

[15] The position that bank records, under the Fourth Amendment, require a search warrant or other judicial process in order to be lawfully obtained by law-enforcement agencies had been rejected by the U.S. Supreme Court in United States v. Miller, 425 U.S. 435 (1976).

Fair Credit Reporting Act of 1970.[16] This statute regulates the preparation and disclosure of consumer reports and investigative consumer reports.[17] While a consumer report may be furnished for various legitimate business needs, disclosure for other purposes requires an order of a competent court. A consumer reporting agency may give identifying information respecting any consumer, limited to his name, address, former addresses, place of employment, or former places of employment, to a government agency. The agency must disclose to the consumer the identity of any recipient of reports on him it has furnished within the 6 months preceding the consumer's request for such information (a 2-year period is specified for a report for employment purposes). An investigative consumer report cannot be prepared unless the consumer is notified; and the person procuring such an investigation must, upon request by the consumer, disclose the nature and scope of the investigation requested.

---

[16] 15 U.S.C. Sec. 1681 et seq.

[17] Section 1681a. includes the following definitions:

"(d) The term 'consumer report' means any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (1) credit or insurance to be used primarily for personal, family, or household purposes, or (2) employment purposes, or (3) other purposes authorized under section 163b of this title..."

"(e) The term 'investigative consumer report' means a consumer report or portion thereof in which information on a consumer's character, general reputation, personal characteristics, or mode of living is obtained through personal interviews with neighbors, friends, or associates of the consumer reported on or with others with whom he is acquainted or who may have knowledge concerning any such items of information..."

The Foreign Intelligence Surveillance Act of 1978.[18] This Act is concerned with the electronic surveillance of agents of foreign powers who engage in activities violating U.S. criminal statutes, including activities associated with international terrorism or sabotage. The Act requires that information concerning a U.S. person acquired from an electronic surveillance conducted under the Act may be used and disclosed by federal officers without the consent of the subject only if specified minimization procedures are followed--for example, "procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 24 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person."

California Financial Privacy Act of 1976.[19] This state law, which is equivalent to the Federal Right to Financial Privacy Act, requires that "... before a financial institution discloses financial records, the agency seeking the records must either receive authorization by the consumer, or obtain an administrative subpoena, a search warrant, or a judicial subpoena. This legislation contains several exemptions to the procedural requirements for access to financial records, yet accomplished its goal of prohibiting financial records of a customer from being released by a financial institution to a governmental agency unless the customer is notified in advance or a

[18] 50 U.S.C. Sec. 1801 et seq.
[19] California Government Code Secs. 7460-7493.

court decides in its discretion that prior notice is not in the public interest and clears the release of the record."[20]

California Court Decisions

In People v. McKunes,[21] it was decided that a government agent's obtaining from the telephone company, without subpoena or other court order, records of telephone calls between a defendant in a criminal proceeding and a third person was a violation of the constitutional right of privacy; as a result, the evidence secured by this act, and its fruits, were inadmissable against the defendant.

The California Supreme Court, in Burrows v. Superior Court,[22] held that any bank statements or copies thereof relating to an accused's accounts obtained by the sheriff and the prosecutor without benefit of legal process but with the consent of the bank involved were acquired as a result of an illegal search and seizure. Northwithstanding the fact that a bank voluntarily relinquished these statements of accounts to the police, the accused had a reasonable expectation of privacy as to these materials.

In People v. Blair,[23] the California Supreme Court held, among other things, that a credit card holder would reasonably expect that

---

[20] Peter H. Behr, "Privacy: To Be or Not To Be, That Is the Question," Pacific Law Journal, Vol. 10, 1979, pp. 669-70. Mr. Behr was a member of the California State Senate who was active in the sponsorship of privacy legislation.

[21] 51 Cal. App. 3d 487 (1975).

[22] 13 Cal. 3d 238 (1974). This decision is reflected in the California Financial Privacy Act of 1976. Burrows is the case in which the California Supreme Court co-opted the concept of "a reasonable expectation of privacy," set forth in Katz v. United States, 389 U.S. 347 (1967). Burrows was expressly predicated on Art. I, Sec. 13 of the California Constitution.

[23] 159 Cal. Rptr. 818 (1979).

information about him disclosed by charges made on a credit card will be kept confidential unless its disclosure is compelled by legal process; and that police acted improperly in obtaining from a hotel, without legal process, a list of telephone calls made from the room of the defendant in a criminal proceeding. The Court ruled that the credit-card information search could not be upheld on the grounds that only lending institutions were prohibited by the California Right to Privacy Act from disclosing financial information about their customers without safeguards set forth in the Act, and that the Act specifically allows a state or local agency to obtain credit reports from other types of financial institutions.

In Tavernetti v. Superior Court,[24] the decision of the California Supreme Court was that a telephone company lineman who reported to the police the contents of a telephone conversation concerning an illegal drug transaction, which he overheard while performing his duties, violated the right to privacy of the accused, according to the Court's interpretation of Article 1, Section 1, of the California Constitution and Penal Code Sec. 630 (The California Invasion of Privacy Act). The Court found that the lineman's disclosure was not related to telephone company business but derived from his perception of his duty to report a crime. The Court concluded that the improperly disclosed information had to be suppressed in the criminal proceeding of the accused; it did not discuss whether the lineman's conduct would have been proper under federal law, as contrasted with California law.

People v. Mejia[25] produced the holding that in the absence of

[24] 22 Cal. 3d 187 (1978).
[25] 157 Cal. Rptr. 233

advance judicial sanction, a motel manager's disclosure to the police of a record of telephone calls made from a motel room violated the right to privacy of the room's occupant. A search warrant based on the illegally derived information was invalid, and the evidence obtained from the search had to be excluded from the proceedings.

In People v. Krivda,[26] the California Supreme Court considered the legality of obtaining information by a warrantless search of trash barrels placed adjacent to the street for collection. It decided that this trash could not be deemed abandoned by the defendants; they therefore had not forsaken any reasonable expectation of privacy as to the contents of the barrels even when examined only after pickup by the refuse truck. The search was unreasonable, and the evidence obtained from it was not admissible.

In People v. Arno,[27] a California appellate court considered the issue of whether the use of optical aids in conducting a physical surveillance constitutes an unconstitutional intrusion upon an individual's right to privacy. The court held that the use of optical aids such as binoculars, telescopes, etc., is not of itself determinative of the admissibility in evidence of the product of the

---

[26] 5 Cal.3d 357 (1971). Krivda was later argued before the U.S. Supreme Court. The Court stated, "... we are unable to determine whether the California Supreme Court based its holding upon the Fourth and Fourteenth Amendments to the Constitution of the United States or upon the equivalent provision of the California Constitution, or both." It remanded the case to the California Supreme Court for clarification, for if Krivda had been decided on independent state grounds, it would not be overturned even if Federal law permitted a warrantless search of the trash. The California Supreme Court certified that the California Constitution furnished an independent ground to support its opinion, which the Court reiterated in its entirety. (See 409 U.S. 33 (1972) and 8 Cal. 3d 623 (1973).)

[27] 90 Cal. App. 3d 505 (1979).

observations, but that the primary determinative factor is the presence or absence of a reasonable expectation of privacy of the person whose conduct, property, or documents is observed. The court further held that reasonable expectation of privacy is tested by the extent to which the person has exposed his conduct, property, or documents to public view by the naked eye. In Arno, where a police officer used 10-power binoculars from a hilltop position to see into an office window on the seventh floor of a building 200 to 300 yards away, the observations were suppressed as an unconstitutional invasion of privacy.

SUMMARY

The past decade has seen a proliferation of legal constraints on the kinds of information gathered in security investigations (as well as on the techniques of gathering, considered more fully in Sec. IV). This growth of constraints reflects the concern with abuses of First Amendment rights and with rights of privacy, as well as continuing attention to Fourth Amendment (search and seizure) rights. The thrust of the new rules is to compel security investigators to obtain approval by an objective magistrate before gathering personal information. With some exceptions, the subjects of security investigations must be notified of the investigative activities as a result of the legal process.

IV. TECHNIQUES OF INFORMATION GATHERING

CONSTRAINTS ON INFORMATION GATHERING TECHNIQUES

The Attorney General's Guidelines

The Attorney General's Guidelines show explicit concern for the techniques of gathering security information. Preliminary investigations are limited to examination of FBI indexes and files; examination of public records and other public sources; examination of federal, state, and local records; inquiry of existing sources of information and use of previously established informants; and physical surveillance and interviews of other persons for the limited purpose of identifying the subject of an investigation. Limited investigations may include physical surveillance and interviews for other than identification purposes, but only when authorized by the Special Agent in Charge.

The Guidelines specifically proscribe recruiting informants or placing them within groups, using mail covers, and electronic surveillance in preliminary or limited investigations. These techniques are permitted in full investigations, but their use is limited.[1] For example, the use of informants must be approved by FBI Headquarters, and their activities must be regularly reviewed; they may not be used to gather information on persons for whom criminal proceedings are pending or to obtain privileged information. Mail covers must be approved by the Attorney General and must conform to postal regulations. Electronic

[1]The Guidelines note with concern that they do not cover "pretext inquiries," "trash covers," and photographic or other surveillance techniques.

surveillance must meet the stringent requirements of Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[2]

A separate set of guidelines for FBI Use of Informants, which became effective in 1976 (see App. B), provides factors that should be weighed in considering the use of informants in an authorized investigation; instructions that the FBI must give to informants; and actions to be taken if the FBI learns of violations of instructions or of law committed by one of its informants.

The Seattle Police Intelligence Ordinance

The Seattle Police Intelligence Ordinance states: "(c) When a police officer knows of two or more techniques to collect restricted information and each would be equally practical and effective, the officer should use the technique which he reasonably believes will have the least adverse impact upon lawful political and/or religious activity." The gathering of restricted information requires written authorization by a higher-ranked officer. Specific criteria must be met to justify the granting of the authorization, and the contents of the authorization must also meet stringent criteria. An authorization does not permit the use of informants or infiltrators to collect restricted information about a victim or a witness to a crime.

The Police Operations section of the Intelligence Ordinance limits the use of infiltrators for gathering restricted information about political, religious, and other specified organizations. Informants must be instructed not to participate in unlawful acts of violence; use

[2] Comparable restrictions on techniques used in gathering foreign intelligence are found in Executive Order 12036, U.S. Intelligence Activities, 43 F.R. 3674, January 24, 1978, which appears in 50 U.S.C. Sec. 401, Cumulative Annual Pocket Part for Use in 1979, pp. 52-54.

unlawful techniques to gather information; initiate a plan to commit criminal acts; or participate in criminal activities of persons under investigation, except with specified approval. Police personnel may not incite any person to commit unlawful violent activity and may not communicate information known to be false or derogatory.

Proposed Operational Guidelines--Los Angeles Police Department PDID

The April 22, 1980, draft of the proposed operational guidelines for the PDID touches upon specific information gathering techniques in only one respect:

> Photographic or electronic surveillance shall not be conducted without the prior authorization of the Commanding Officer. Such authorization will be given only when deemed necessary to accomplish the public disorder intelligence mission. Photographic surveillance will be approved in the following instances:
>
> (1) To identify persons who, either as individuals or as members or associates of groups or organizations, are involved in acts of violence or other violations of law; or
>
> (2) To provide evidence of such violations of law; or
>
> (3) To identify individuals or groups who may pose a threat to the safety of persons who hold, or are candidates for public office, and to the safety of other persons in public life for whom this Department may be called upon to provide personal security escorts ...

The statement of the mission of the PDID does specify that intelligence information may be collected only through lawful means and sources.

Procedures--Public Security Activities of the NYPD Intelligence Division

The current NYPD guidelines mandate the use of only lawful information gathering techniques that minimize interference with the legitimate exercise of civil rights. In addition, they specifically address the techniques of undercover agents, photographic surveillance,

and electronic surveillance. The use of an undercover agent (infiltrator) requires approval of the First Deputy Commissioner or his special designee, and approval must meet the criterion of reasonable necessity. The agent must be shown to have adequate training for the undercover assignment, and regular reports on his or her activities must be given to the First Deputy Commissioner or his special designee.

Photographic surveillance requires prior authorization by the Commanding Officer of the Intelligence Division, by the Chief of the Inspectional Services Bureau, or by the First Deputy Commissioner. It can be used only:

- To identify persons who, either as individuals or as members or associates of groups or organizations, are involved in acts of violence or other violations of law;
- To obtain evidence of such violations of law; or
- To identify individuals or groups who may pose a threat to the safety of persons who hold or are candidates for public office.

Electronic surveillance can be conducted only in strictest conformity with court-authorized warrants and with the rules and procedures governing the entire NYPD.

FBI POLICIES, PRACTICES, AND PROCEDURES[3]

Because of the FBI's central role in domestic security, its publicly reported policies, practices, and procedures concerning intelligence gathering techniques are of particular importance.

---

[3] This section is based on an FBI letter response of June 13, 1978, to questions from the Senate Committee on the Judiciary, which stemmed from the April 25, 1978, hearings on the FBI Charter legislation. (Reprinted in FBI Statutory Charter, Hearings before the Committee on the Judiciary, United States Senate, 95th Congress, Second Session, April 20 and 25, 1978, Part 1, pp. 75-83).

Undercover Agents

The authority to use undercover agents resides with the Special Agent in Charge in each field division of the FBI. In special situations, such as long-term operations, approval must be granted by FBI Headquarters. Virtually all undercover activities are closely coordinated, with the U.S. Attorney holding prosecutorial power over the investigation being conducted. Undercover operations must observe the restraints of the First, Fourth, Fifth, and Sixth Amendments to the U.S. Constitution, pertinent statutes and executive orders, U.S. Department of Justice regulations and guidelines, and internal FBI administrative and operational procedures.

Mail Covers

Mail covers may be used only when a full investigation has been authorized by FBI Headquarters. Part 831 of the Postal Manual of the U.S. Postal Service sets forth regulations authorizing the Assistant Postmaster General, Inspection Service (Chief Postal Inspector), to administer mail covers at the request of enforcement agencies. In security investigations, as defined in the Manual of Investigative Operations and Guidelines, mail cover requests must include complete names and addresses of individuals or organizations to be covered and any pertinent additional information, such as the attorney of record for the subject and whether or not the subject is under indictment. The approval of the Attorney General is required for the use of mail covers.

Electronic Surveillance

Electronic surveillances are authorized either by an order of a U.S. district court, under the provisions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, or by a person participating in the communication. The Attorney General's policies are stated in the Agent's Manual for Conduct of Electronic Surveillance under Title III of Public Law 90-351 and the Manual for Conduct of Electronic Surveillance under Title III of Public Law 90-351. These departmental booklets together provide step-by-step procedures.

Under Title III, authorization for interception of wire or oral communications is limited to specified crimes, including serious offenses related to sabotage and to riots. The internal FBI procedures for applying for an electronic surveillance warrant are sufficiently stringent that only one of the first 1,050 applications made after the enactment of Title III was denied.

When interception is performed on the basis of a party's consent and only telephones are involved, the Attorney General allows the Special Agent in Charge to authorize surveillance if the U.S. Attorney concurs and opines that no legal entrapment would result. With certain emergency exceptions, prior approval must be obtained from the Attorney General for a participant in the communication to conceal on his person or premises a transmitter or recorder.

Physical Surveillance

The FBI Manual of Investigative Operations and Guidelines distinguishes between fixed and mobile surveillance and, within these two categories, between close (i.e., subject under surveillance at all

times) and loose (spot checks as appropriate) surveillance. Surveillance logs composed of chronological surveillance notes must be maintained, and all written data relating to physical surveillance must be submitted to the field office daily by the agents involved. Specific Headquarters authority must be obtained to use FBI employees other than agents on surveillances (except in counterintelligence investigations). Surveillance in important cases requires personal, on-the-scene supervision by the Special Agent in Charge. The manual does not provide detailed descriptions of surveillance techniques; rather, it states that "practical experience in this activity is the best teacher."[4]

Other Techniques

There are no formal written procedures for use of trash covers by the FBI. The agency position is that under federal law, FBI agents may seize trash placed out for collection without a warrant and without infringing on the constitutional rights of the person who so placed the trash, since this property has been abandoned and hence is not protected by the Fourth Amendment. (California's position, as promulgated in People v. Krivda, is far more restrictive.)

Also, no formal procedures have been written for FBI interviews. However, general procedures are given in the Manual of Investigative Operations and Guidelines. The Attorney General's Guidelines for Domestic Security Investigations allow interviews during preliminary, limited, and full investigations.

Finally, the FBI has no formal written procedures for access to third-party or other-agency records.[5] The FBI has generally had

[4] MIOG, Part III, 9-1(2), p. 1037.

[5]As an exception, the FBI Manual of Investigative Operations and Guidelines does provide agent guidance for use of the Fair Credit Reporting Act to obtain information. MIOG, Part III, 23-2, p. 1439, 1/31/78.

access to state motor vehicle records and to state and local law-enforcement records, but access to records of other federal agencies is strictly governed by the Privacy Act.

THE LEGAL FOUNDATIONS OF ELECTRONIC SURVEILLANCE

The Fourth Amendment's proscription against arbitrary intrusion by police is the core protection of the privacy of communications. Legal restraints on electronic surveillance have evolved in terms of what constitutes a "search" under the Fourth Amendment. This development is traced below through a series of legal landmarks.[6]

1928: Olmstead v. United States, 277 U.S. 438. The Supreme Court held that Fourth Amendment protections did not extend when interception was accomplished without physical trespass on the target's home or business. The Court concluded that the Fourth Amendment protected only material things, i.e., the premises, not the communication.

1934: The Federal Communications Act, Pub. L. No. 73-416 (codified in various sections of 47 U.S.C.). For 34 years, Section 605 of the Act served as the basic source of Federal wiretap law. Apparently prompted by Olmstead, Section 605 provides, in part, that

> No person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any

[6] This chronology, which does not purport to be exhaustive, is based primarily on I. S. Shapiro, "The Foreign Intelligence Surveillance Act: Legislative Balancing of National Security and the Fourth Amendment," Harvard Journal on Legislation, Vol. 15:1, 1977, pp. 127-139; and J. Courtney, "Electronic Eavesdropping, Wiretapping and Your Right to Privacy," Federal Communications Bar Journal, Vol. 26, No. 1, 1973, p. 7 et seq. Other sources include "Title III and National Security Surveillance," Case Comment, Boston University Law Review, 56: 853-875, Summer, 1978, pp. 776-777; and the American Jurisprudence and California Jurisprudence legal encyclopedias.

> person; ... and no person having received such intercepted communication or having become acquainted with the contents, substance, purport, effect, or meaning of the same of any part thereof, knowing that such information was so obtained, shall divulge or publish the existence, contents, substance, purport, effect or meaning of the same or any part thereof, or use the same or any information therein contained for his own benefit or for the benefit of another not entitled thereto...

1937: Nardone v. United States, 302 U.S. 379 (Nardone I). The Supreme Court decided that Section 605 of the Federal Communications Act applied to wiretapping by federal and state officials as well as by private persons. Evidence obtained from wiretapping in violation of Sec. 605 became inadmissible in Federal courts and would not support a criminal conviction.

1939: Nardone v. United States, 308 U.S. 338 (Nardone II). The Supreme Court held that "fruits" of wiretaps, in addition to the contents of the intercepted messages, were inadmissible in federal courts.

1940: U.S. Justice Department Policy Developments. The Justice Department discontinued all wiretapping activity in March 1940. Soon thereafter, it adopted a position that Sec. 605 prohibited only tapping followed by divulgence, not tapping alone; and that divulgence did not occur when one member of government communicated wiretap information to another member of government. In particular, government wiretapping was permissible if the information obtained was disseminated within government for law enforcement. (This interpretation justified electronic surveillance for 27 years. In 1974, it was judicially rejected in United States v. Butenko, 494 F.2d 593 (3rd Cir.), cert. denied, 419 U.S. 881.)

A Presidential Memorandum to the Attorney General opined that Nardone did not apply to "grave matters involving the defense of the Nation." The Attorney General was authorized "in such cases as you may approve ... to secure information by listening devices [directed at] the conversations or other communications of persons suspected of subversive activities against the United States, including suspected spies" and was admonished "to limit these investigations so conducted to a minimum and to limit them insofar as possible to aliens."

1942: Goldman v. United States, 316 U.S. 129. Section 605 was held to protect the means of communication, not the secrecy of communications; that is, the message was safeguarded only during the course of its transmission. Where there is no trespass, there is no interception. This case was to eavesdropping what Olmstead was to wiretapping.

1946: Expansion of U.S. Justice Department Wiretapping Authority. Presidential acceptance was granted a Justice Department request for wiretapping authority without the limitations of the 1940 Presidential Memorandum.

1952: Schwartz v. Texas, 344 U.S. 199. The Supreme Court decided that wiretap evidence obtained by state agents could be divulged in state courts, notwithstanding Sec. 605.

1952: On Lee v. United States, 343 U.S. 747. The Supreme Court found no constitutional violation when incriminating statements were picked up by a "wired for sound" acquaintance of the defendant, given no physical trespass into the latter's home.

1952: Change of Justice Department Eavesdropping Policy. The Attorney General decided that trespassory microphone surveillance violated the Fourth Amendment and should not be authorized.

1954: Change of Justice Department Eavesdropping Policy. The Attorney General authorized the FBI to conduct trespassory microphone surveillance in the national interest.

1957: Benanti v. United States, 355 U.S. 96. The Supreme Court decided that wiretap evidence gathered by state agents in violation of Sec. 605 was inadmissible in federal court.

1957: Rathbun v. United States, 355 U.S. 107. The Court interpreted the so-called "consent doctrine" and found that the consent of any party sufficed for interception and divulgence of a telephone conversation, viz., "Each party to a telephone conversation takes the risk that the other party may have an extension telephone and allow another to overhear the conversation."

1961: Silverman v. United States, 365 U.S. 505. In deciding a case where a spike microphone had been inserted into a party wall and made contact with a duct serving the defendant's entire home, the Court implicitly held that words as well as material things could be unconstitutionally seized.

1963: Lopez v. United States, 373 U.S. 427. The Court held that where a government agent used a pocket wire recorder (rather than a concealed microphone as in On Lee), the defendant's transcribed incriminating conversation was not unconstitutionally seized and divulged. There was no trespass and the recording revealed only what the defendant willingly disclosed to the agent.

1963: Wong Sun v. United States, 371 U.S. 471. The Court declared that "it follows from our holding in Silverman ... that the Fourth Amendment may protect against the overhearing of verbal statements as well as the more traditional seizures of 'papers and effects'."

1967: Berger v. State of New York, 388 U.S. 41. The Court found New York's permissive eavesdropping statute to be constitutionally deficient. It specified that, to be constitutional, a federal or state statute must (1) authorize eavesdropping only on a showing of probable cause; (2) describe specifically what is to be seized; (3) provide for notice to the subject; (4) have a determined limitation on the time of search; and (5) make a mandatory return to the magistrate specifying what was seized.

1967: Katz v. United States, 389 U.S. 347. In Katz, the Supreme Court overturned Olmstead and Goldman, abandoning the property approach to the Fourth Amendment. The Court said that "the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not the subject of Fourth Amendment protection ... But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." It rejected the trespass doctrine by holding that "the Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth ..."

1968: Title III of the Omnibus Crime Control and Safe Streets Act, Pub. L. 90-351. This legislation is discussed in detail on pp. 51-53.

1972: United States v. United States District Court, 407 U.S. 297 (the Keith case). This case provided a partial answer to the question of whether in national security situations the President had inherent powers to justify disregard of the warrant procedure otherwise required by the Fourth Amendment. The Court ruled that the Fourth Amendment demands a warrant procedure in domestic security cases.

1973: United States v. Baxter, 492 F.2d 150 (9th Cir.), cert. denied, 416 U.S. 940 (1974). The Court, relying on federal case law that an expectation of privacy protected by the Fourth Amendment attaches only to the contents of a telephone conversation, not to the fact that a conversation took place, held that warrantless acquisition of telephone company toll call records is not unconstitutional.

1975: Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir.), cert. denied, 96 S. Ct. 1684 (1976). The Court decided that warrantless electronic surveillance directed against domestic organizations whose conduct affected foreign affairs violates the Fourth Amendment.

1978: United States v. New York Telephone Company, 434 U.S. 159. The Supreme Court held that Title III does not affect Court authorizations of pen registers that record telephone numbers called. Pen registers do not intercept because they do not acquire the contents of communications. The Court reiterated this position in the case of Smith v. Maryland, 47 U.S. L. Week (June 20, 1979), again stating that there is no reasonable expectation of privacy in the phone numbers that a person calls.[7]

---

[7] California law is more restrictive in the matter of pen registers, which appear to violate Penal Code Sec. 631 and possibly 632. Consent of the telephone subscriber (and the telephone company) seems to be the only authorization legally recognized, whether or not there is any intention to intercept a message. (See People v. Jones, 30 Cal.

1979: Dalia v. United States, 99 S.Ct. 1622. This Supreme Court decision held that under federal law, courts may authorize electronic surveillance that requires covert entry into private premises to install the necessary equipment and there need not be a specific statement in the authorization that the federal court approves of the covert entry.[8]

The relevant parts of Title III of the Omnibus Crime Control and Safe Streets Act[9] respecting techniques of gathering intelligence information are summarized in the following.

Title III, the first federal law specifically regulating electronic surveillance, amended Sec. 605 of the Federal Communications Act of 1934 by limiting the applicability of its wiretapping provisions to radio communications. The Omnibus Crime Control and Safe Streets Act prohibits all forms of wiretapping and eavesdropping, with certain exceptions. It forbids the procuring of persons to wiretap or eavesdrop and the disclosure or use of information obtained through such surveillance. Violations can be punished by fines of up to $10,000 and prison terms of up to five years.

Under Title III, there are four specific classes who may lawfully intercept oral or wire communications under special circumstances: (1)

App. 3d 852 (1973), app. dism., California v. Jones, 414 U.S. 804 (1973); and "Pen Registers," Peace Officer Law Report, California Department of Justice, September 1978, pp. 12-17.)

[8] California law is again more restrictive. The surveillance conduct approved in Dalia is not permissible under Penal Code Secs. 630-631.2 and various judicial decisions. California has no provision for judicial authorization of covert entries for electronic surveillance. Evidence so obtained, even if by federal agents acting under a valid federal court order, would not be admissible in California courts. (See People v. Jones.)

[9]18 U.S.C. Sec. 2511 et seq. pertain here. The Act, effective in 1968, was successively amended in 1970, 1971, and 1978.

the wireline common carrier, when interception is necessary to render service and to protect its rights and property; (2) the FCC, when discharging its monitoring responsibilities under the Communications Act; (3) a person acting under the color of law who has the prior consent of a party to a communication; and (4) a private person who has the consent of a party and intends no criminal, tortious, or injurious result.

The Attorney General (or a specially designated assistant) is empowered to authorize application for a federal court order permitting eavesdropping (wiretapping or electronic "bugging") in the investigation by federal law-enforcement agencies of certain enumerated offenses. State or county prosecutors may also apply to a state judge for an order authorizing electronic surveillance when the interception of communications may provide evidence of one of a broad set of offenses, as long as such action is not forbidden by state statute.

An interception order may be issued only if the judge determines that specific grounds exist to justify eavesdropping--ordinarily, normal investigative procedures must have failed or the government must show that methods different from interception are unlikely to succeed or are too dangerous.

Wiretapping or bugging may continue only as long as necessary and no longer than 30 days. Thirty-day extensions are possible if the judge makes new findings sufficient to uphold an original authorization. No more than 90 days after application for a wiretap order and its denial or after termination of a wiretap period if one is approved, the judge must notify the parties involved, giving the dates and fact of the application, its approval or disapproval, and the interception or non-interception of communications.[10] Information obtained as a result of

---

[10] This provision has been criticized by law-enforcement agencies

an authorized surveillance is admissible in any criminal proceeding and can be divulged in the performance of law enforcement. Emergency interception without prior judicial authority is permitted under certain circumstances, provided the government applies for a court order within 48 hours of commencing the interception.

Failure to comply with the provisions of Title III makes the unauthorized eavesdropper subject to criminal penalties and gives the victim a civil cause of action for invasion of privacy. Finally, Title III contains a "national security disclaimer" stating that the Congress has neither authorized nor prohibited national security electronic surveillance.

A number of state laws pertaining to electronic surveillance (e.g., those of Kansas, Minnesota, Nebraska, New Hampshire, New Mexico, South Dakota, Virginia, and Wisconsin) follow federal law closely.[11] California law goes well beyond the requirements of federal law.[12]

INFORMANTS AND UNDERCOVER AGENTS

Historically, informants and (to a lesser degree) undercover agents have been a fruitful source of domestic security intelligence. Legal and administrative constraints on the use of informants and agents have emerged slowly and have tended to be concentrated in certain areas.

---

because it tends to endanger informants still involved in a security investigation.

[11] As characterized in Compilation of State & Federal Privacy Laws, op. cit.

[12] California Penal Code sections 630-637.2 forbid wiretapping and electronic eavesdropping except by law-enforcement officers. Consent of all parties is the general California rule, but with some law-enforcement exceptions. No wiretap warrants can be obtained.

The case of White v. Davis, discussed earlier, raised the issue of whether the Los Angeles Police Department could lawfully conduct a covert intelligence gathering activity involving undercover officers as registered students at state universities. The California Supreme Court held that such activities could be sustained only if the defendant "can demonstrate a 'compelling state interest' which justifies the resultant deterrents of First Amendment rights and which cannot be served by alternative means less intrusive on fundamental rights."

The Attorney General's Guidelines proscribe the recruiting or placing of informants within groups for preliminary or limited investigations. They may be used in full investigations, but only with the approval of FBI Headquarters. These activities must be regularly reviewed and they may not be used to gather information on persons for whom criminal proceedings are pending, nor may they be used to obtain privileged information. The Guidelines for FBI Use of Informants (reproduced in App. B) provide factors that the FBI should weigh in considering the use of informants; instructions to be given to informants; and actions to be taken in the event an informant commits violations of instructions or of law.

The Seattle Police Intelligence Ordinance also limits the use of infiltrators for obtaining restricted information from within and about political, religious, and other specified organizations. Informants must be instructed not to participate in unlawful acts of violence; use unlawful techniques to gather information; initiate a plan to commit criminal acts; or participate in criminal activities of persons under investigations, except with specified approval.

Under federal constitutional law,[13] law-enforcement agencies have broad discretion in determining when, where, how, and against whom informants may be used for domestic intelligence gathering. The U.S. Supreme Court has thus far declined to hold that the use of informers per se is unconstitutional or that the decision to use informers should be subject to prior judicial review.

Fourth Amendment Considerations. The admissibility into evidence of a target's incriminating statements that were "seized" by an informant or undercover agent has repeatedly been an issue before the courts. The cases of On Lee v. United States, 343 U.S. 747 (1952) (an undercover agent "wired for sound"), Lopez v. United States, 373 U.S. 427 (1962) (an undercover agent with a wire recorder), Osborn v. United States, 383 U.S. 323 (1966) (an informer with a tape recorder), and Hoffa v. United States, 385 U.S. 293 (1966) (direct testimony by a government informer based on memory and notes) resulted in the defendant's statements being admitted into evidence, on the basis that the Fourth Amendment does not protect a wrongdoer's misplaced belief that a person in whom he confides his wrongdoing will not reveal it. These decisions were called into question following Katz v. United States, 389 U.S. 347 (1967), and the Supreme Court cleared the air in United States v. White, 401 U.S. 745 (1971), a case that involved a government informant carrying a concealed radio transmitter. The Court held that Katz did not disturb the results in On Lee or the earlier cases. It reiterated that the Fourth Amendment does not prohibit

---

[13] This discussion borrows from M. L. Perschetz, "Domestic Intelligence Informants, the First Amendment and the Need for Prior Judicial Review," Buffalo Law Review, Vol. 26, 1976-77, pp. 173-208.

testimony about a defendant's statements to an informant, howsoever the latter records or transmits the conversation. Thus, the use of informants by law-enforcement agencies continues to be considered outside of the purview of the Fourth Amendment and therefore not subject to any warrant requirement or other sort of prior judicial review.

Another Fourth Amendment issue concerns the use of information gained by informants in establishing probable cause to support the issuance of a search or arrest warrant. The courts, in a series of cases, have ruled that hearsay will support a finding of probable cause but the informant must be found credible and the basis for believing him credible must be shown.[14]

Another related issue concerns the so-called informant's privilege, i.e., the withholding of his identity in criminal proceedings in which his information is used. The courts have generally upheld the evidentiary rule of most states that police officers need not, except on matters of a suspect's guilt or innocence, be required to disclose an informant's identity. An informant's name need not be disclosed to the magistrate from whom a warrant is sought or to the judge at a hearing on the suppression of the informant's evidence unless such disclosure is necessary to show his reliability, but it may be required prior to trial if it is necessary to the defendant's case on its merits.[15] Needless to say, the prospect of identity disclosure is a serious constraint on

---

[14]The cases include McCray v. Illinois, 386 U.S. 300 (1967); Aguilar v. Texas, 378 U.S. 108 (1964); Spinelli v. United States, 393 U.S. 410 (1969); and United States v. Harris, 403 U.S. 573 (1971).

[15] Cases relating to this issue include McCray v. Illinois, 386 U.S. 300 (1967); Roviaro v. United States, 353 U.S. 53 (1957); Rugendorf v. United States, 376 U.S. 528 (1964); and Scher v. United States, 305 U.S. 251 (1937). California law, which is relatively favorable toward the disclosure of an informant's identity, states that

> "Where otherwise proper, the accused may require disclosure of an informant's identity in advance of trial. The basic issue in

the use of informants by law-enforcement agencies and is a source of considerable defense leverage to obtain dismissal of charges in lieu of such disclosure.

Fifth Amendment Considerations. The Supreme Court held in Hoffa that the Fifth Amendment privilege against self-incrimination is not violated when an informant elicits incriminating verbal information from a suspect, in the absence of coercive tactics or custodial interrogation.

---

determining whether disclosure of an informer's identity is required is one of constitutional due process, and lies in the balance of the public interest in protecting the flow of information to law enforcement officials against the individual's right to prepare his defense. Although the government is generally privileged to withhold the identity of informers, the privilege must give way when it comes into conflict with the fundamental principle that a person accused of a crime is entitled to a full and fair opportunity to defend himself, and, in such cases, the balance is struck in favor of the defendant, and disclosure must be ordered upon pain of dismissal. Thus, although the statute inhibiting the examination of a public officer concerning confidential communications made to him may protect the identity of an informer the privilege of nondisclosure must yield to the right of the defendant to disclosure of the informer's identity where the latter was a participant in the alleged crime. Moreover, there is no privilege of nondisclosure if disclosure is relevant and helpful to the defense or essential to a fair determination of the case. Nor is the defendant's right to disclosure precluded by the fact that the prosecution has produced strong eyewitness testimony of the defendant's guilt.

"The reasons for requiring disclosure at the trial also require disclosure at the preliminary hearing, for the defendant has the right at the hearing to cross-examine the prosecution's witnesses and to produce witnesses in his own behalf. It follows that the defendant, in a proper case, is entitled to be given the name of the informer on demand; and if a proper demand is made, refusal of the request is reversible error. And when in a proper case the accused seeks disclosure on cross-examination, or on timely motion before trial, the prosecution must either disclose the identity or incur dismissal. Again, when the prosecution seeks to show reasonable cause for a search by testimony to communications from an informer, and the defendant seeks disclosure of the informer's identity, either the identity must be disclosed or the testimony must, on the defendant's proper motion, be stricken ..." (Sec. 964 of 18 California Jurisprudence 3d).

Sixth Amendment Considerations. Early cases indicated that the mere presence of a government agent when client and counsel were conversing could violate the right to counsel guaranteed by the Sixth Amendment. However, the Supreme Court in Hoffa (1966) and later in Weatherford v. Bursey, 429 U.S. 545 (1977), rejected the notion that such invasion of the attorney-client relationship has this force without regard to the way in which the intercepted conversation is used in the proceedings. Thus in the great majority of security investigations, the use of informers to obtain information about matters within the attorney-client relationship would not be invalidated by Sixth Amendment restrictions. Since surveillance of this type almost always occurs well in advance of formal proceedings and is often unrelated to any specific criminal activity, law-enforcement agencies have broad discretion in this area. Only when formal proceedings have commenced, when there is more than the mere presence of the informer within the legal defense camp, and when the information reported to the government relates to the specific charge against the defendant are courts mandated by the Sixth Amendment to find a violation of the right to counsel.[16]

Due Process Considerations. The due process clauses within the Fifth and Fourteenth Amendments are violated by police practices that

---

[16] In the case of Barber v. Municipal Court, 24 Cal. 3d 742 (1979), the California Supreme Court found that the gathering of information by an informant involved an "intrusion, through trickery of the law enforcement agent in the confidential attorney-client conferences," on the right to counsel guarantee of the California Constitution. In consequence, the Court dismissed the charges. Court decisions have recognized the right to communicate in absolute privacy with one's attorney. In addition, numerous California statutes are designed to protect the confidentiality of the attorney-client relationship, for example, Business and Professions Code Sec. 6068, Evidence Code Sec. 954, and Penal Code Sec. 636.

are shockingly unfair. While the Supreme Court consistently declares that due process constitutes a barrier to certain police activities, it has been reluctant to invoke this standard. Indeed, no court has yet found an informant's activities to be unconstitutional on the grounds of violating due process.

Judicial Supervision Considerations. Federal courts may go beyond minimum constitutional requirements (which are applicable even to state convictions) in the supervisory administration of federal criminal justice. Even though due process is not expressly violated, federal courts may grant remedies whenever the administration of justice is sufficiently tainted. It appears, however, that a high degree of misconduct would have to be proved before a federal court would invoke this remedial power. (See, however, the dissenting opinion in Hoffa by then-Chief Justice Warren.)

First Amendment Considerations. The relevance of First Amendment rights to certain police informant activities was addressed by the California Supreme Court in White v. Davis. Although the First Amendment probably serves as the most severe constraint on the use of informants in some domestic security contexts, the scope of its protection has not been clearly articulated by the U.S. Supreme Court.

In the landmark case of Laird v. Tatum, 408 U.S. 1 (1972), which involved a nationwide intelligence plan adopted by the U.S. Army in response to civil disorders during the summer of 1967, the U.S. Supreme Court held that no justiciable controversy (i.e., no basis for a lawsuit, no legal cause of action) was presented by a claim that the mere existence of an intelligence gathering and distributing system created an unconstitutional chilling effect on First Amendment rights,

where the plaintiffs were not specific targets of government action. However, the Court refrained from ruling on the question of the propriety or desirability of the type of surveillance at issue in Laird, holding only that its challengers did not allege sufficient injury to their rights. Although the First Amendment's role as a barrier against the use of informants by the government was not settled in Laird, a lower state court ruled that "the police violate the First Amendment when they engage in an unrestrained surveillance operation calculated to stifle the willingness of people to exercise those preferred freedoms of speech, association, and assembly" (People v. Collier, 376 New York Supplement, 2d Series, 984 (1975)). To avoid violations of the First Amendment and the right to privacy, "an infiltrator may be planted in a group only when the police have articulable reasons to believe or suspect that criminal activity is afoot, and the operation should continue only until sufficient evidence is obtained to warrant an arrest." (People v. Collier, p.988.)

Legal and administrative constraints on the use of informants leave considerable latitude. The prospect of identity disclosure through, for example, judicial discovery in criminal proceedings or freedom-of-information laws, provides a more immediate constraint.

ENTRAPMENT

Entrapment or the use of agents provocateurs[17] refers to police conduct that can be the basis for an affirmative legal defense in a criminal proceeding. Though the courts of almost every U.S.

[17] An agent provocateur is one employed to associate himself with members of a group or with suspected persons and by pretended sympathy with their aims or attitudes incite them to some action that will make them liable to apprehension and punishment.

jurisdiction have long recognized the issue of entrapment by police, they are deeply divided in their views. The U.S. Supreme Court has articulated the opposing views in several leading cases.

In the first defense of entrapment considered by the Supreme Court (Sorrells v. United States, 287 U.S. 435 (1932)), the majority adopted the "subjective or origin-of-intent" test under which entrapment is established only if (1) governmental investigation and inducement overstep the bounds of permissibility, and (2) the defendant did not harbor a preexisting criminal intent. A finding that the defendant was predisposed to commit the offense would defeat the defense, i.e., vindicate the police technique. Under this test, because entrapment bears on guilt or innocence, it is an issue for the jury to decide. By contrast, the minority or objective test in Sorrells considers the defendant's conduct or predisposition to be irrelevant and holds that the purpose of the entrapment defense is solely to deter police misconduct. It follows that the judge alone can decide whether entrapment occurred, and thereby whether to afford protection against impermissible law-enforcement methods.

These opposing positions were reiterated in Sherman v. United States, 356 U.S. 369 (1958), with the majority again adopting the subjective test and the minority maintaining that permissible police activity does not vary for different defendants. More recently, in United States v. Russell, 411 U.S. 423 (1973), the Supreme Court reviewed the entrapment defense and again, by a 5-4 vote, declined to overrule the subjective test adopted in Sorrells.

The entrapment concept had a separate development in the state courts. In California, until the case of People v. Barraza, 23 Cal.3d

675 (1979), the test for entrapment reflected a position between the subjective and the objective: California courts did not permit the introduction of highly prejudicial evidence of subjective predisposition of the accused, yet they did base the existence of entrapment upon whether the intent to commit the crime originated with the police or with the accused. Barraza marked the adoption of a new and objective test of entrapment: Was the conduct of the law-enforcement agent likely to induce a normally law-abiding person to commit the offense? Official conduct that does no more than offer a suspect the opportunity to act unlawfully is permissible, but the police or their agents may not pressure a suspect by overbearing conduct such as badgering, cajoling, importuning, or other affirmative acts that could induce a normally law-abiding person to commit a crime.

Because entrapment is a legal defense in a criminal proceeding, it is not strictly a constraint on police activities in a security investigation whose purpose is primarily to gather information. But to the extent that criminal prosecutions are at least a by-product of such investigations, entrapment is an impermissible technique.

V. INFORMATION HANDLING

The constraints on the handling of security information are probably the most diverse and complex of any relating to information gathering and use. In this section, we shall examine legislative, judicial, and administrative constraints, and we shall review the nature and role of freedom-of-information and privacy legislation.

CONSTRAINTS ON HANDLING OF INTELLIGENCE INFORMATION

The Attorney General's Guidelines[1]

The Attorney General's Guidelines permit the FBI to disseminate information gathered in a security investigation to other federal agencies when the information falls within the investigative jurisdiction of those agencies; when such dissemination may assist in preventing the use of force or violence; or when the dissemination is required by statute, by interagency agreement approved by the Attorney General, or by Presidential Directive. Similarly, the FBI may disseminate such information to state and local law-enforcement agencies within whose investigative jurisdiction the information falls, when dissemination may assist in preventing the use of force or violence, or when it may protect the integrity of a law-enforcement agency. The FBI is mandated to refer by-product information about serious crimes obtained within a security investigation to appropriate law-enforcement

---

[1] An exhaustive presentation on FBI information and telecommunication systems and FBI records management policies is given in "FBI Statutory Charter--Appendix," Part 3, Hearings before the Subcommittee on Administrative Practice and Procedure of the Committee on the Judiciary, United States Senate, 95th Congress, Second Session.

agencies. The Guidelines do not limit FBI authority to warn any individual whose safety or property is threatened, according to information the FBI gathers. Finally, the FBI is required to maintain records of disseminations of domestic security information outside the Department of Justice.

Within an unspecified number of years after closing a security investigation, the FBI must destroy all information obtained during that investigation, as well as all index references to it, or it must transfer the information and references to the National Archives and Records Service.[2]

The Seattle Police Intelligence Ordinance

A substantial portion of the Seattle Intelligence Ordinance is devoted to rules for the handling of restricted information. These rules include the following:

- Information indexed for ready retrieval must be regularly reviewed and retained only if it is relevant to law-enforcement activities or required by law.
- Disclosure is limited to records open for public inspection; to arrest information disclosed to the public for law-enforcement purposes; and to information needed by criminal agencies and by certain specified persons and regulatory agencies.

---

[2] On their effective date (March 10, 1976), the Guidelines left the length of the retention period for domestic security information open to later determination. According to the GAO followup report of November 9, 1977, op. cit., the Attorney General's Guidelines committee intended to recommend the destruction of intelligence files five years after an investigation is closed without prosecution and ten years after an investigation that leads to prosecution.

- o Disclosure of information from records closed to public inspection is limited to relevant facts and materials, with certain exceptions under law.

The Intelligence Ordinance does specify what communications and materials are confidential, what materials are open to public inspection, and what is excluded from its restrictions.[3]

The Ordinance directs that restricted information shall not be transmitted to another agency unless that agency has a need that would support an authorization order, subpoena, court order, or statutory provision; or unless a local investigation or judicial proceeding is to be served. Logs of such transmissions must be maintained. The Ordinance defines the functions of a Criminal Intelligence Section, particularly with respect to criminal intelligence information handling, and it provides for an auditor to audit the files, logs, records, and indices of information regulated by the Intelligence Ordinance and to notify any person about whom restricted information may have been collected in violation of the Intelligence Ordinance and who would have a civil remedy under its provisions.

Standards and Procedures of the Los Angeles PDID

Administrative constraints on intelligence handling are included in the Standards and Procedures for the Los Angeles PDID.[4] These

[3] For example, information on the name of an informant which is privileged from disclosure in a court of law is confidential; information about anticipated political or religious events is open to public inspection; and the collection of information about police conduct by the Department of Internal Investigations Section is excluded from application of the Ordinance.

[4] Publicly reported by the Los Angeles Board of Police Commissions in April 1975 and adopted in December 1976. One commissioner recently recounted: "In 1973 a series of meetings was

guidelines are concise but comprehensive. They define which individuals and organizations may be the subjects of intelligence files; how these files are physically constituted; standards and procedures for recording and storage of information in files; permissible sources of file information; standards and procedures for dissemination of file information; review and auditing of files; and file security.

The standards limiting the scope of the intelligence data files were adopted to avoid abuses in domestic security investigations, especially infringements upon constitutionally protected rights. The inclusion of individuals and organizations in the files is based on their link with unlawful acts disruptive of public order or of legally protected civil rights. The files themselves are organized by the type of data they contain: individuals, organizations, source materials, significant dates, and potential victims. The form of the files is specified to be card files, and the information entries are also specified. Information sources are restricted to (1) standardized intelligence reports generated by police investigations, containing an identification of the original source and an indication of the reliability of the information; (2) publications and other public

---

initiated between the Police Commission, the Chief of Police, and the Director of the Office of Special Services to review the Public Disorder Intelligence Division. This review ultimately resulted in the destruction of close to two million outdated or irrelevant index cards on individuals and organizations. After subsequent public hearings and review by a special committee of the Bar and the City Attorney, a formal set of guidelines, outlining standards and procedures for PDID, was adopted in December, 1976. It is important to remember that the Commission and the Department pioneered this area; the guidelines went beyond any existing judicial or legislative requirements of the time. Guidelines concentrated on the retention and maintenance of files--requiring six separate levels of review for new entries and four separate levels of review for additions to existing files."

sources; and (3) communications from other law-enforcement agencies, again with identification of the source and an indication of reliability.

Dissemination of intelligence file information within the LAPD and to outside law-enforcement agencies is on a restrictive need-to-know basis, defined within these standards. A dissemination log must be kept.

File cards must be reviewed at least annually by supervisory personnel, and unnecessary or irrelevant information must be purged, given approval by the commanding officer. A file that is dormant for seven years must be purged unless there is good cause for retaining it. The subject's becoming a fugitive would be expected to constitute good cause, but in practice this has not been invariably the case. A quarterly audit of the PDID and its files must be made by a member of the Board of Police Commissioners.

Procedures for Public Security Activities of the NYPD

Public Security officers of the NYPD must designate the source of all intelligence information they receive and must provide a statement of informant reliability in cases where the information derives from an informant. The raw information must then be evaluated by an analysis section before any reporting, recording, filing, or dissemination occurs. Information deemed to lack substantial relevance to the Public Security mission is destroyed, with the concurrence of the Chief Analyst or the Commanding Officer of the Intelligence Division. The intelligence information that is retained is then formally classified according to

- Importance (i.e., seriousness of subject matter)

  A. Major
  B. Intermediate
  C. Minor

- Time priority (i.e., urgency of police action or attention)

  1. Very high (within 24 hours)
  2. High (within 24 to 72 hours)
  3. Medium (within 3 to 7 days)
  4. Low (more than 7 days)
  5. For information only

- Source reliability

  H. Highly reliable
  R. Reliable
  U. Unknown

- Content substantiation

  S. Substantiated
  N. Not substantiated

After the information has been evaluated and classified, the need for additional data may be indicated. All available data on the subject being investigated are then assembled and analyzed. The analysis section assesses causes and significance of past events and projects future developments. It is the responsibility of the Commanding Officer of the Intelligence Division either to accept and report the analysis; to require its revision; or to direct further investigation.

Once intelligence information has been evaluated and found to meet specified criteria, it is recorded on index cards that are color-coded by year to facilitate periodic review. Each card contains the source of the information and its classification.

The NYPD Intelligence Section guidelines provide criteria and procedures for the dissemination of Public Security information,

distinguishing between intradepartmental and extradepartmental dissemination. They proscribe the formal or informal dissemination of Public Security information to nongovernmental individuals or agencies. Special, more restrictive criteria and procedures are provided for the dissemination of surveillance photos.

The Commanding Officer of the Intelligence Division, the Public Security Coordinator, the Intelligence Division Legal Analyst, and the Chief Analyst must frequently review the subjects of Public Security attention to determine whether information collection and retention should continue. In addition, every Public Security file card must be reviewed at least once within two years of its initial filing to determine whether it should be kept active, placed in a dormant file for reevaluation within two years, or purged and destroyed. Similar review procedures are provided for surveillance photos.

California Criminal Intelligence File Guidelines

In addition to the above procedures and guidelines, there is a body of handling constraints that are not confined to a single agency but have broad applicability at the federal or state level.

In 1978, the California Department of Justice, Division of Law Enforcement, published a comprehensive set of guidelines for criminal intelligence files maintained by law-enforcement agencies within the state.[5] A criminal intelligence file is defined to be one that consists of stored information on the activities and associations of individuals and groups known or suspected to be involved in criminal acts or in the threatening, planning, organizing, or financing of criminal acts. (While this definition encompasses files derived from

[5] Republished in April 1980.

security investigations, it is customary to separate "criminal" files from "domestic security" files. Nevertheless, the guidelines should be relevant to both.)

The guidelines cover the content of criminal intelligence files, the criteria for retaining information within them, an assessment of source reliability and content validity, classification of the information security level, identification of information sources, quality control, dissemination, purging, and file security.

Files may not contain religious, political, or sexual information not related to criminal conduct. Furthermore, to help protect the confidentiality of criminal intelligence files, criminal history record information (which is subject to specific audit and dissemination restrictions designed to protect privacy) is also excluded.

The guidelines distinguish between a permanent criminal intelligence file and a temporary file for information not meeting the permanent-file criteria but having enough potential validity to be retained for one year, or longer if a compelling reason exists. The input for a permanent file must pertain to an identifiable individual, organization, business, or gang that has been involved, is involved, or is suspected of being involved in one or more specified criminal activities, including, for example, manufacture, use, or possession of explosive devices for purposes of fraud, intimidation, or political motivation.

The guidelines direct that information retained in intelligence files must be evaluated for source reliability and content validity, using specified qualitative indexes. Information must be classified in terms of security level, as confidential, sensitive, or restricted (in

descending order of sensitivity). Dissemination criteria and release authority are keyed to the security class.

The guidelines encourage individual law-enforcement agencies to establish their own criteria to define when the source of filed intelligence information should be identified within the file. Similarly, the agencies are asked to adopt their own dissemination rules based on the evaluation of source reliability and content validity, on security classification, and on the requestor's need-to-know and right-to-know.

Procedures for quality control review of filed information are not set forth in the guidelines; criteria are given for file purging but not for its frequency.

Constraints on the handling, and in particular, the dissemination of criminal-history record information are generally statewide. Such information receives unique treatment, in part because of Law Enforcement Assistance Administration (LEAA) regulations covering privacy and security of criminal-history information, issued to implement sections of the 1973 amendment to the Omnibus Crime Control and Safe Streets Act.[6] The states have tended to implement these guidelines by statute in order to retain federal funding for criminal-justice information systems. The resultant handling constraints have been criticized as being inimical to security investigations, as indicated in a Congressional staff report:[7]

---

[6] 28 Code of Federal Regulations Part 20.

[7] "Security Clearance Procedures in the Intelligence Agencies," Staff Report, Committee on Oversight, Permanent Select Committee on Intelligence, U.S. House of Representatives, September 1979, p. 17.

> Problems in this area arise primarily from guidelines established by the ... LEAA. LEAA defines "criminal history record information" as information collected by criminal justice agencies (courts, government agency, or subunit thereof involved in the administration of criminal justice) on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information on other criminal charges, and any disposition arising therefrom, sentencing, correctional supervision and release.
>
> These guidelines on Criminal Justice Information Systems place no restrictions whatsoever on the dissemination of conviction data, arrests made within the year of an inquiry, and arrests where charges are actively pending. However, the guidelines state specifically that policies regarding dissemination of nonconviction data by law enforcement agencies is left to states, and that is where the problem occurs. Because LEAA guidelines allow all 50 states to develop their own policies on dissemination of criminal justice information to non-law enforcement agencies, a very scattered pattern exists. Much useful information is denied intelligence agency investigators.

But another Congressional report[8] faults the LEAA for the opposite reason, listing LEAA pressures designed to bring local and state procedures into conformance with its interpretation of the federal requirements as a principal factor in the erosion of law-enforcement intelligence.

CONSTRAINTS ON THE HANDLING OF CRIMINAL HISTORY INFORMATION IN CALIFORNIA

According to a compilation of statutes and regulations pertaining to California criminal record security, privacy, and confidentiality prepared by the California Department of Justice in 1978,[9] the

---

[8] "The Erosion of Law Enforcement Intelligence and Its Impact on National Security," op. cit., p. 2.

[9] "California Criminal Record Security, Statutes and Regulations," Department of Justice, Criminal Records Security Unit, Security and Compliance Bureau, Division of Law Enforcement, Sacramento, California, January 1978.

relevant provisions appear in the state penal, administrative, government, education, welfare and institutions, labor, and evidence statutory codes. For example, the California Administrative Code contains the following provisions:[10]

> (a) Each authorized agency[11] shall designate specific personnel to release criminal offender record information[12] pursuant to these regulations. Only designated personnel may release such information.
>
> (b) Criminal offender record information may be released, on a need-to-know basis, only to persons or agencies authorized by court order, statute, or decisional law to receive criminal offender record information.
>
> (c) Each authorized agency shall keep a record of each release of California Department of Justice rap sheets or information derived therefrom. The record shall be retained and available for inspection for a period of not less than three years from the date of release ... (footnotes added)

These provision suggest that in California there would generally be no denial of criminal-history information requested by any agency lawfully conducting a security investigation.

Section 11105, California Penal Code, which deals with state summary criminal history information prepared by the Attorney General,[13] specifies the persons and agencies (in California) to whom

---

[10] Sec. 703, Article 1, Subchapter 1, Chapter 1, Title II, Administrative Code.

[11] An "authorized person or agency" means any person or agency authorized by court order, statute, or decisional law to receive criminal offender record information. (From Sec. 700, id.)

[12] "Criminal offender record information" means records and data compiled by criminal justice agencies for purposes of identifying criminal offenders and of maintaining as to each such offender a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation, and release. Such information shall be restricted to that which is recorded as the result of an arrest, detention, or other initiation of criminal proceedings or of any consequent proceedings related thereto. (Sec. 700, id.)

[13] State summary criminal-history information is the master record of information compiled by the Attorney General pertaining to the

the Attorney General must furnish state summary criminal-history information--the courts, the district attorneys, the probation officers, the parole officers, a public defender or attorney of record when representing a person in a criminal case, the subject of the history, etc. It also specifies the persons and agencies (not necessarily in California) to whom the Attorney General may furnish state summary criminal history information. These include peace officers of the United States and of other states, statutorily authorized public officers of the United States and of other states, the courts of the United States and of other states, etc. These requestors must show a compelling need for the information.

THE ROLE OF FREEDOM-OF-INFORMATION AND PRIVACY LAWS

The federal and state freedom-of-information and privacy laws impose even broader legal constraints on the handling of domestic security information. This body of statutory law, together with the case law interpreting it, has had probably the most pervasive and profound effects on domestic security information gathering. It is also the main source of the commonly supposed constraints on gathering this information.

The importance of freedom-of-information and privacy laws (and their interactions) in terms of domestic security derives from their impact on

---

identification and criminal history of any person (e.g., name, date of birth, physical description, date of arrests, arresting agencies and booking numbers, charges disposition). It does not refer to records and data compiled by criminal-justice agencies other than the Attorney General, nor does it refer to records of complaints to, investigations conducted by, or records of intelligence information or security procedures of the Office of the Attorney General and the Department of Justice. (Sec.11105(a)(i) and (II),PC.)

- o Access by the public to personal information held by law-enforcement agencies and to information about those agencies.
- o Access by subject individuals and organizations to personal and organizational information held by law-enforcement agencies.
- o Access by law-enforcement agencies to personal and organizational information held by other government agencies or by agencies or individuals outside the government.

These issues are central to domestic intelligence information handling, and ambiguities in the privacy laws and the complex interactions among them have led to significant uncertainty about access to and disclosure of intelligence information, its sources, and the techniques of gathering it. As a result, there has been considerable litigation of unpredictable outcome, and this has exacerbated the effects of freedom-of-information and privacy laws on government conduct in general and on domestic security investigations in particular.

Federal Freedom-of-Information Laws[14]

The Freedom of Information Act (FOIA), enacted in 1966 and amended in 1974,[15] is concerned with the creation of information files by

[14] See C. Y. Singleton and H. O. Hunter, "Statutory and Judicial Responses to the Problem of Access to Government Information," Detroit College of Law Review, 1:51, 1979, pp. 52-53, 69-70; "Access to Information? Exemptions from Disclosure under the Freedom of Information Act and the Privacy Act of 1974," Willamette Law Journal, Vol. 13, 1976, pp. 154-158; "FOIA and Privacy Act Interface: Toward a Resolution of Statutory Conflict," Loyola University Law Journal , Vol. 8, 1977, pp. 578-80, 586.

[15] Pub.L. No. 89-487, 80 Stat. 250, 5 U.S.C. Sec. 552 (1966), as amended, 5 U.S.C. Sec. 552 (Supp. 1976).

federal agencies and the rights of the public to obtain access to such information. (The FOIA is summarized in Appendix C, and selected provisions from it are reproduced there.)

The FOIA requires federal agencies to make available all information held by them to any person who requests it, unless the information falls within one of nine narrowly construed exemptions. Moreover, any reasonably segregable portion of any record must be available to any person after exempt portions have been deleted.

The seventh exemption, which is most relevant to law-enforcement information, exempts from mandatory disclosures matters that are

> investigatory records compiled for law enforcement purposes, but only to the extent that production of such records would (A) interfere with enforcement proceedings, (B) deprive a person of a right to a fair trial or an impartial adjudication, (C) constitute an unwarranted invasion of personal privacy, (D) disclose the identity of a confidential source and, in the case of a record compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security investigation, confidential information furnished only by the confidential source, (E) disclose investigative techniques and procedures, or (F) endanger the life or physical safety of law enforcement personnel....

The burden is on a law-enforcement agency to justify its denial of record disclosure if the requestor sues in federal district court to compel disclosure. The Act does not require that information in any exempt category be kept confidential; disclosure is left to agency discretion.

The seventh exemption was amended in 1974 to overrule a series of decisions by the Court of Appeals for the District of Columbia that permitted indefinite withholding of investigatory files regardless of

the unlikelihood or impossibility of future criminal proceedings. In its original form, the exemption permitted agencies to withhold "investigatory files compiled for law enforcement purposes except to the extent available by law to a party other than an agency." The amending narrowed the exemption by requiring proof that disclosure would interfere with either pending or imminent enforcement proceedings. (By contrast, the addition of item (C) in 1974 broadened the seventh exemption significantly.) In sum, federal investigatory files for law-enforcement purposes,[16] which generally include files of federal domestic security investigations, are exempted from mandatory disclosure, provided one of six specific harms is shown. The courts have tended to construe the language of the first of these harms as meaning an ongoing enforcement proceeding or investigation.

Federal law-enforcement agencies tend to rely on the seventh exemption to avoid disclosure of materials that are not specifically investigatory files--for example, manuals of investigatory techniques and procedures, only parts of which may be exempt because of national security classification. Yet, federal case law interpreting the FOIA has weakened denial of disclosure of readily segregable, unclassified portions of an investigative manual because of the harm of disclosing investigative techniques and procedures. Specifically,[17]

---

[16] According to the Attorney General's 1974 FOIA Amendments Memorandum, "investigatory records are those which reflect or result from investigative efforts. Law enforcement includes not merely the detection and punishment of law violation, but also its prevention."

[17] This material was developed by William R. Harris, The Rand Corporation.

- The 1974 Amendments to the FOIA compel release of any reasonably segregable portions of otherwise exempt "records." (See 5 U.S.C. Sec. 552(b).)
- The duty to release reasonably segregable portions of classified documents is affirmed in Founding Church of Scientology v. Bell, 603 F.2d 945 at 951 (Ct. App. D.C. Cir., 1979).
- The Court of Appeals for the District of Columbia Circuit, which hears most of the appeals on this issue, has consistently limited the exemptions for law-enforcement agency manuals to those specified in the FOIA.
- The burden of proof in justifying a denial on the basis of the seventh exemption rests with the government agency. (See Dept. of the Air Force v. Rose, 425 U.S. 352 (1976); Ollestad v. Kelley, 573 F.2d 1109 (Ct. App. 9th Cir., 1978); Fonda v. CIA, 434 F.Supp. 498 (D.C.D.C., 1977).)
- There are precedents in both directions: Disclosure by the CIA was ordered in Marks v. CIA, 590 F.2d 997 at 1004 (Ct. App. D.C. Cir., 1978); disclosure by the Drug Enforcement Administration was ordered in Slacet v. Bensinger, 605 F.2d 899 at 901, 903 (Ct. App. 5th Cir., 1979); and nondisclosure by the FBI was upheld in Librach v. FBI on the grounds that disclosure of procedures for an informant relocation program would jeopardize the effectiveness of informants as an investigative technique.

- o Manuals that pertain exclusively to internal housekeeping and personnel practices must be distinguished from manuals that are of public interest, since the former affect the decision to investigate or prosecute. (See Cox v. U.S. Department of Justice, 601 F.2d 1 (Ct. App. D.C. Circuit, 1979), in which the court sustained an order for the release of the Manual for U.S. Marshals, with limited exemptions.)
- o The intent of the FOIA is to provide a mechanism for public disclosure, not a mechanism to suppress information, as affirmed in Scherer v. Kelley, 584 F.2d 1970 (1978).

Thus, despite the ostensible shield of the seventh exemption, there is uncertainty about whether or not a law-enforcement agency can deny disclosure of unclassified portions of investigative manuals.

State-Level Freedom-of-Information Laws

According to the Privacy Protection Study Commission,[18] nearly every state has a freedom-of-information or open-public-records statute which requires that state government records be available for public inspection.[19]

---

[18] The Report of the Privacy Protection Study Commission, "Privacy Law in the States," Appendix 1, July, 1977.

[19] There is no uniform definition of a "public record." Some states have incorporated the common law definition into their statutes, designating as public records those records required by law to be maintained. Other states have expanded the definition to include all records made or received by government agencies in the course of transacting official business. Several state statutes are more comprehensive still, encompassing any record or information that relates to the conduct of government or is in the possession of the state. Under a narrow definition, some law-enforcement records might not be interpreted as public records.

A public record must be disclosed to anyone who asks for it unless another statutory provision permits or requires that it be withheld. Like the federal FOIA, many state open-records statutes exempt records whose disclosure would result in an unwarranted invasion of personal privacy or is otherwise prohibited by law. Typically, open-records statutes exempt specific types of records. Law-enforcement records are customarily given a permissive exemption. For example, Sec. 6254(f) of the California Government Code, states:

> ... nothing in this chapter shall be construed to require disclosure of records that are: ... (f) Records of complaints to or investigations conducted by, or records of intelligence information or security procedures of, the office of Attorney General and the Department of Justice, and any state or local police agency, or any such investigatory or security files compiled by any other state or local police agency, or any such investigatory or security files compiled by any other state or local agency for correctional, law enforcement, or licensing purposes, except that local police agencies shall disclose the names and addresses of persons involved in, or witnesses other than confidential informants to, the incident, the description of any property involved, the date, time, and location of the incident, the statements of all witnesses, other than confidential informants, to the persons involved in the incident, or an authorized representative thereof, an insurance carrier against whom a claim has been or might be made, any person suffering bodily injury or property damage as a result of the incident caused by arson, burglary, fire, explosion, robbery, vandalism, or a crime of violence as defined by subdivision (E) of Section 13960, unless the disclosure would endanger the safety of a witness or other person involved in the investigation, or disclosure would endanger the successful completion of the investigation or a related investigation....

While this exemption on its face seems very broad, its application has been narrowed by judicial construction. In State Division of Industrial Safety v. Superior Court, 43 C.A. 3d 778 (1974), the court found that the term "law enforcement" used in this section refers to the

enforcement of penal statutes and that the section does not protect from disclosure or discovery official files or information not involving a definite prospect of criminal law enforcement. It also found that the term "investigatory files" is limited in its application to situations where the prospect of future enforcement proceedings is concrete.

A related issue concerns whether exempt information held by law-enforcement agencies is open to discovery in a criminal proceeding when this information appears to be essential to a fair trial and the alternative to its discovery is dismissal of criminal charges.

Finally, some states have enacted statutes that override their open-records statutes and provide for the confidentiality of certain government-maintained records. We have already noted the restrictions imposed by many states on the disclosure of criminal history information, usually in response to regulations promulgated by the LEAA and applying to all state criminal-justice information systems receiving LEAA funds.

Federal-Level Privacy Laws

The Privacy Act of 1974[20] is concerned with safeguarding personal privacy by limiting the collection, maintenance, use, and dissemination of personal information by federal agencies.[21] The Act imposes a variety of requirements on systems of records containing information about individuals that are accessed by personal identifiers. For example, each agency

---

[20] Pub.L. No. 93-579, 88 Stat. 1896 (1974), 5 U.S.C. Sec. 552a (Supp. V, 1975).

[21] The Act's restrictions apply only to the federal government, covering all executive departments, the military, independent regulatory agencies, government corporations, and government-controlled corporations. They do not apply to Congress, the federal courts, the District of Columbia, or the governments of U.S. territories or possessions.

- o Must publish annually a notice of the existence and character of its records systems.
- o Must supply specified items of explanatory information to individuals about whom personal information is being collected for its record systems.
- o Must store only information relevant and necessary to accomplish a required purpose of the agency and must maintain the information with accuracy, timeliness, and completeness.
- o Must not disclose information except by written consent or upon request of the subject, except in specified circumstances--e.g., to agency employees to perform their duties; when required by the FOIA; for a routine use; or to another agency for a civil or criminal law-enforcement activity given an appropriate request.
- o Must keep an accurate accounting of each disclosure for at least five years, available to the subjects of the disclosures.

Individuals have the right of access to their records, as well as the right to copy and request amendments. Civil and criminal remedies are provided through legal actions in federal district courts to individuals who are improperly denied access to or amendment of their records or who are adversely affected by improper disclosure of records or other agency violations of the Act. (See Appendix D for a fuller summary of the Act, including several key provisions concerning exemptions and comments about these provisions.)

The Act contains three types of exemptions relating to domestic security information:

- o Conditions of disclosure, i.e., conditions under which an agency may disclose a personal record without prior written consent of the subject. (Subsection 3(b) of the Act; 5 U.S.C. 552a (b))
- o General exemptions, i.e., characteristics of a system of records that enable an agency head to promulgate rules exempting the system from most of the requirements of the Act. (Subsection 3(j); 5 U.S.C. 552a(j))
- o Specific exemptions, i.e., characteristics of a system of records that enable an agency head to promulgate rules exempting the system from specified requirements of the Act. (Subsection 3(k); 5 U.S.C. 552a(k)).

The statutory provisions for each of these exemptions are given in Appendix D.

The dissemination of security records among law-enforcement agencies, even records not covered by one of the above exemptions, would probably be covered by one of several conditions permitting disclosure without consent of the individual involved:

- o Disclosure to officers and employees of the agency that maintains the record who need the record in the performance of their duties.
- o Disclosure for a routine use, i.e., for a purpose compatible with the purpose for which it was collected.
- o Disclosure to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the

> United States for a civil or criminal law-enforcement activity if the activity is authorized by law and if the head of the agency or the instrumentality has made an appropriate written request.

The Privacy Act thus appears not to prevent the transfer of federal law-enforcement information on individuals among federal and other law-enforcement agencies.

The general and specific exemptions--as stated in Subsections (j) and (k), respectively--come into play when the issue concerns a subject's access to his own security records.

No law-enforcement record system is automatically exempt from the requirements of the Privacy Act. But an agency head can readily obtain an exemption by determining that a record system qualifies for exemption under subsection (j) or (k) and filing an appropriate notice in the Federal Register. An agency whose principal function pertains to law enforcement may exempt a system of records under Subsection (j) if the records consist of

- Information compiled for the purpose of identifying suspects and offenders, consisting only of identifying data and notations of arrests, charges, and the events of ensuing criminal proceedings.
- Information compiled for the purpose of a criminal investigation that is associated with an identifiable individual.
- Reports on identifiable subjects compiled at any stage of the process of criminal law enforcement.[22]

[22] The FBI Manual of Investigative Operations and Guidelines

Although Subsection (j) enumerates those sections of the Act to which exemption is supposedly inapplicable, in practice, this subsection, supplemented by the conditions of disclosure, produces immunity from virtually all of the Act's restrictions.[23] For example, Subsection (j) does not provide exemption from the provisions of Subsection (b) concerning notice to the subject and his consent for disclosure. But also under Subsection (b), any law-enforcement agency can acquire personal records without notice and consent, provided the agency head requests the records in writing and certifies that they will be used for law-enforcement purposes.

Subsection (j) does not provide exemption from the requirement of making and retaining an accounting of disclosures as mandated in Subsection (c), yet Subsection (c) relieves law-enforcement agencies of the requirement of making this accounting available to the subject at his request. And Subsection (j) does not exempt a law-enforcement agency from the requirements of Subsection (e) limiting the maintenance of records describing an individual's exercise of First Amendment rights, but Subsection (e) itself allows such a record to be maintained if it is pertinent to and within the scope of a law-enforcement activity.

---

states: "FBI files containing information compiled for a criminal investigation, including determining possible violations of the espionage and related statutes, are presently exempt from the access provisions of the Privacy Act; however, pursuant to Title 28, Code of Federal Regulations, section 16.57(b), a discretionary release can be made of such records under the FOIA. This includes FBI criminal, counterintelligence, and domestic security-type investigations." (MIOG: Part I, 190-2(3), p. 901, January 31, 1978.)

[23] These arguments are set forth in "The Privacy Act of 1974: An Overview and Critique," Washington University Law Quarterly, Vol. 1976, Fall 1976, pp. 696-698.

Subsection (k) enables a law-enforcement agency to exempt investigatory records compiled for law-enforcement purposes (beyond the materials exempt under Subsection (j)) from provisions requiring the agency to provide notice and access to a subject of the records. There is a limitation on this exemption of investigatory materials, however:

> ... if any individual is denied any right, privilege, or benefit that he would otherwise be entitled to by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

The subject of domestic security records might use this provision as a basis for overturning a denial of access. It runs counter to the otherwise broad immunity from the requirements of the Privacy Act that Congress appears to have conferred on federal criminal law-enforcement agencies. And, on its face, it is a source of uncertainty about whether security information can be fully and reliably shielded from disclosure.

State-Level Privacy Laws

We have already summarized the status of privacy law in the states as respects individually identifiable information held by government agencies (see pp. 25-28).

INTERACTION BETWEEN PRIVACY AND FREEDOM-OF-INFORMATION LAWS

The interaction of privacy and freedom-of-information laws constitutes a substantial source of uncertainty as to whether law-enforcement agencies can be compelled to disclose investigatory material, including domestic security information, to subjects, to third parties, or to the public.

The Federal Level

The interaction of the Privacy Act of 1974 and the FOIA has been summarized by one analyst as follows:[24]

> The FOIA and the Privacy Act provide two different avenues by which individuals can request information from government agencies. While each has its advantages and disadvantages, the important point is that the FOIA is the parent act and ultimately governs access to information. The Privacy Act is relegated to the backseat when a successful disclosure request is made under the FOIA. Thus, even if a record has been declared exempt under the Privacy Act, access may still by sought under the FOIA with its attendant nine exemptions. If the record is available under the FOIA, access must be granted, the Privacy Act notwithstanding.
>
> Generally, an individual seeking information regarding a third party must proceed under the FOIA, since the Privacy Act blocks access to such information. To obtain access under the FOIA, it is necessary to justify intrusion into the third party's privacy by showing that disclosure is not a clearly unwarranted invasion of personal privacy. If disclosure is not a clearly unwarranted invasion of personal privacy or prohibited by any other FOIA exemption, then the file must be made available pursuant to the FOIA and section (b)(2) of the Privacy Act. Qualifying in this manner renders the Privacy Act exemptions from disclosure ineffectual to impede access to record systems containing information regarding third parties.

---

[24] "Access to Information?" op. cit., p. 140. Here, the term "available" means that disclosure is mandatory because the material does not fall within one of the exemptions. The Privacy Act bars disclosure unless the requesting party qualifies under one of eleven conditions of disclosure. (For example, release of information about newly arrested persons would be permitted under the "routine use" exemption.) Subsection (b)(2) says simply that disclosure is not barred by the Privacy Act when it is required by the FOIA.

This analysis appears to apply not only to third-party access but also to the subject's seeking disclosure, since this would not be an invasion of his privacy. Thus it would seem that a law-enforcement agency must rely almost entirely on the seventh exemption of the FOIA, rather than on its record exemptions under the Privacy Act, to avoid disclosure of investigatory records. Furthermore, the courts are constrained to construe the seventh exemption narrowly.

An opposing view of the interaction between the Privacy Act and the FOIA is given in the following extract:[25]

> Subsection (q) of the Privacy Act expressly prohibits agencies from relying on the exemptions of the FOIA to withhold information otherwise available to the requestor under the Privacy Act. However, neither Act contains any provision dealing with the situation where an individual requests his or her records under the FOIA when the agency has exempted them from disclosure under the Privacy Act. In addition to claiming that portions of the requested record are exempt under the FOIA, the agency may contend that under the Privacy Act its exemption of the system containing the record renders the entire record "specifically exempted from disclosure by statute" and therefore unavailable under the FOIA's exemption 3. An agency might use this argument to withhold a record from its subject even though none of the other FOIA exemptions applied.

This statement seems also to apply to a third-party request under the FOIA, but it is uncertain whether this position would prevail in court.[26]

---

[25] "FOIA-Privacy Act Interface," op. cit., p. 586 (footnote omitted).

[26] If a requestor under the Privacy Act fails to also make a separate request under the FOIA, he may not be able to contest in court the withholding of requested records, since the agency could have exempted not only the record system under the Privacy Act but also the court's jurisdiction.

Until case-by-case court decisions and legislative amendments clarify the joint effects of these laws, it will not be possible to assess the risk that certain investigatory records may have to be disclosed sometime in the future. This uncertainty has been blamed for stifling domestic security investigations by federal law-enforcement agencies,[27] prompting the destruction and purging of investigatory files, the revision of purging schedules, the modification of storage, security, and access practices for handling information files, and the use of new or modified audit procedures. Files of intelligence information gathered in an investigation undertaken without a clear expectation that criminal proceedings will ensue are subject to probably the highest degree of uncertainty about the possibility of disclosure. For example, an investigation of a pattern of conduct by a group that speaks of violence but apparently has not provided probable cause or at least a reasonable suspicion that a federal crime has been committed or is pending may never be subject to disclosure.

Federal agencies have reportedly used various devices to subvert or avoid these laws.[28] For example, sensitive information has been filed in record systems that are not accessed by personal identifiers and are thus not covered by the Privacy Act. (The existence of record systems outside of the Privacy Act need not be published.)

---

[27] See, for example, "The Erosion of Law Enforcement Intelligence," op. cit.

[28] Much of this discussion is taken from R. R. Belair, "Agency Implementation of the Privacy Act: Impact on the Government's Collection, Maintenance and Dissemination of Personally Identifiable Information," The John Marshall Journal of Practice and Procedure, Vol. 10:465, 1977, pp. 487-488.

Agencies and individual officials have also created temporary or informal files to lessen the risk of having to disclose information gathered in a "fishing" investigation that lacked a probable-cause basis.

Another practice, attributed particularly to law-enforcement agencies, is to keep information in open investigatory files after an investigation is terminated. This avoids the disclosure requirements of the FOIA because of the exemption for information in investigatory files whose disclosure would compromise an enforcement proceeding.

Finally, federal agencies may store data, including personal information, in "data havens"--systems maintained by organizations that are not subject to the Privacy Act or the FOIA, such as government agencies outside of the executive branch.[29]

The State Level

Five of the seven states having omnibus privacy or fair-information-practice acts have attempted to anticipate and resolve conflicts between privacy and freedom-of-information legislation.[30] The Arkansas and Utah fair-information-practices acts specifically may not be interpreted so as to limit access to information available under their respective open-records statutes. Similarly, the Connecticut and Massachusetts privacy acts state that their provisions limiting disclosures do not apply to information whose disclosure is otherwise authorized. And the Minnesota privacy law establishes a procedure for categorizing

[29] The U.S. Supreme Court recently held that the telephone conversation transcripts of a former Secretary of State, which had been removed from the State Department and deposited with the Library of Congress, were beyond the reach of the Freedom of Information Act.

[30] "Privacy Law in the States," op. cit.

information about individuals as "public," "private," or "confidential," and each of its state agencies is responsible for deciding in which category its records fall. Information that would be available under the state's open-records statute is defined as "public" information. For example, arrest information that is reasonably contemporaneous with the arrest or incarceration is public information. If state or federal law specifies that certain information shall not be available to the individual to whom it pertains, it is "private" information. Information that, by statute, is neither publicly available not accessible by the individual is "confidential" information. If there is no explicit statutory authority to categorize a record as private or confidential, the agency must categorize it as public, although there is a provision for emergency exceptions.

CRIMINAL PROCEEDINGS

Domestic security investigations do not necessarily culminate in criminal proceedings; they may serve, for example, to prevent the attempt of contemplated criminal acts. But law-enforcement agencies generally do seek successful prosecutions following security investigations, in the belief that conviction and imprisonment are the best available response to terrorists and their ilk. The handling of security investigation information as evidence is central to criminal proceedings, and some aspects of security information handling serve as impediments to successful criminal prosecutions.

A major source of difficulty for prosecutors is the exclusionary rule devised by the U.S. Supreme Court as a sanction against police misbehavior in violating Fourth Amendment proscriptions against unreasonable search and seizure.[31] Increasing difficulties are imposed

[31] See "Impact of the Exclusionary Rule on Federal Criminal

on prosecutors as the courts recognize an ever-widening set of situations in which the police cannot gather admissible evidence without first invoking judicial process, usually in the form of a warrant issued by a neutral magistrate. We have already noted a variety of California court decisions that touch on this issue (see pp. 35-38). Specifically, McKunes (1975), Burrows (1974), Blair (1979), Tavernetti (1978), Mejia (1979), and Krivda (1971, 1973) assert the requirement of prior legal process in the circumstances of telephone-call records in the hands of the telephone company, bank statements in the hands of the bank, credit card records in the hands of a hotel, telephone conversations overheard by a telephone lineman, telephone-call records in the hands of a motel, and trash barrels placed in the street for trash collection, respectively.

Undoubtedly, court decisions clarifying the scope of warrant requirements to achieve admissibility of evidence increase pressure on the police to invoke legal process before certain searches, seizures, and arrests. Nevertheless, the time-consuming and technical nature of the warrant process continues to inhibit police use. This may be particularly so in security investigations, where police activity is sometimes felt to be appropriate when probable cause to believe that a crime has been committed is lacking. Efforts by defense counsel to traverse (i.e., deny the facts of) warrants or to obtain disclosure of informants whose statements support their issuance also inhibit police use of warrants.

Prosecutions," report by the Comptroller General of the United States, prepared at the request of Senator E. M. Kennedy, GGD-79-45, April 19, 1979, for a concise summary of the rationale of the exclusionary rule of evidence and for empirical evidence that its impact on federal criminal prosecutions is not as substantial as is widely believed.

Discovery by the defense is another area that lends itself to abuse and thereby to undue constraints on prosecutors.[32] As a matter of legal principle, an accused in a criminal prosecution is generally entitled to discover all relevant and material information in the possession of the prosecution that will assist him in the preparation and presentation of his defense. In particular, the government is generally privileged under statutory law to withhold the identity of informants, but this privilege yields when it conflicts with the constitutional due-process principle that an accused person is entitled to a full and fair opportunity to defend himself. When disclosure of an informant's identity is relevant and helpful to a determination of guilt or innocence, a court will order disclosure upon pain of dismissal. Defense counsel may unreasonably pursue a course of discovery motions to obtain informant indentities or other sensitive information, not only to complicate and delay criminal proceedings but in the hope that police unwillingness to disclose may result in rulings favorable to their motions for dismissal of charges.

A discovery-related legal development that may exacerbate the difficulty of successful prosecution is the widening use of the defense of discriminatory law enforcement. The California Supreme Court, in Murgia v. Municipal Court, 15 Cal.3d 286 (1975), ruled that a criminal defendant may object to the maintenance of the prosecution on the grounds of deliberate invidious discrimination in the enforcement of the law, and that this defendant is not limited to a civil suit for damages or injunctive relief. Furthermore, the Court held that on the basis of

---

[32] Appendix E reviews the fundamentals of criminal discovery, emphasizing its relevance to intelligence disclosure.

this defense, criminal defendants may obtain a discovery order directing the prosecutor to produce information relevant to the claim that various penal statutes were discriminately enforced. Clearly there is a potential for abuse of such motions where defense counsel makes excessive demands for sensitive police records in cases where a defense of discriminatory enforcement is unlikely to prevail under any circumstances. Unwillingness to accept a discovery order in such cases may result in dismissal of a proceeding in which a conviction might otherwise be virtually certain.

Adoption of the objective test of entrapment or agents provocateurs by some state courts, in contrast to the use of the federal subjective test, presents another difficulty for prosecutors. The objective test concentrates on police conduct alone; the defendant's conduct or predisposition is irrelevant. In the subjective test, under which the entrapment defense is less likely to prevail, entrapment depends upon whether the intent to commit the crime originated with the police or with the accused.

Finally, prosecutorial difficulties are increased in states whose laws are more stringent than those of the federal jurisdiction because a defense based on the government's intrusion into the attorney-defendant conferences may suffice for dismissal of charges. By contrast, federal case law, as set forth, for example, in Hoffa and Weatherford, rejects the notion that a mere invasion of the attorney-client relationship, without regard to how the intercepted conversation is used in the criminal proceedings, violates the Sixth Amendment. In the same vein, prosecutors are inclined to view prison rules concerning attorney-inmate communications as excessively protective and facilitative of criminal acts.

VI. REPORTING AND CONTROLLING SECURITY INVESTIGATIONS

In earlier sections, we have noted a variety of report and control requirements that affect the conduct of security investigations, including

- The need for police to invoke legal process as a prerequisite to obtaining many types of third-party-held records, conducting searches, intercepting communications, etc.
- The monitoring and control of communication interceptions by a judge granting an interception order under, say, Title III.
- The duties imposed on agency officials to maintain confidentiality of investigatory files under privacy and freedom-of-information laws.
- Audits of intelligence files imposed by statute or regulation.

This final section focuses explicitly on provisions for reporting and control of security investigations.

The Attorney General's Guidelines

The Attorney General's Guidelines permit the initiation of preliminary investigations by FBI field offices without authorization from a higher level but limit them to a duration of 90 days unless extended by a written authorization from FBI Headquarters. Limited investigations must be authorized in writing by a Special Agent in Charge or by FBI Headquarters, again with written authorization by Headquarters needed to extend the investigation beyond 90 days.

Full investigations must be authorized by FBI Headquarters. The use of informants must be similarly approved and then reviewed at intervals of 180 days or less. Mail covers must be approved by the Attorney General or his designee, initially or upon extension, with postal regulations being observed. Electronic surveillance must conform to the specifications of Title III. FBI Headquarters must periodically review the results of full investigations, and the Department of Justice must review them at least annually. Full investigations may not be continued for more than one year without written approval of the Department. Preliminary, limited, and full investigations may be terminated at any time by the Attorney General, his designee, or FBI Headquarters.

Periodic reports of preliminary investigations that involve a 90-day extension and of limited investigations must be made to the Department of Justice. FBI Headquarters must maintain and provide to the Department on request a statistical analysis of preliminary and limited investigation activities, broken down by field office. The progress of full investigations must be reported by the FBI to the Department of Justice 90 days after such investigations are initiated, and at least annually thereafter while the investigations continue.

In addition to controlling the dissemination of information gathered in security investigations and mandating the maintenance of dissemination records, the Guidelines include specifications for retention and subsequent destruction or archival storage of investigative records.

The Guidelines for Use of Informants specify the factors that must be weighed in justifying the use of informants in an authorized domestic security investigation, the instructions that must be given, and actions that must be taken when an informant violates his instructions or the law by any act, whether or not it is connected with his assignment.

The General Accounting Office follow-up report on FBI domestic intelligence operations (1977, op. cit., p. 45) states the following conclusions:

> The Department and FBI have better control over intelligence activities because current policies (1) more clearly distinguish preliminary from full investigative phases in terms of permissible techniques and duration and scope of investigation and (2) require regular reporting by field offices to FBI headquarters and the department.
>
> While the guidelines have gone a long way toward providing direction and control, certain aspects are subject to varying interpretation as personnel within the Department of Justice and FBI change. The extent and nature of the controls themselves could change since they are not specifically mandated by statute.

Recommendations by the GAO for changes in direction and control of FBI domestic security operations are currently being considered in Congressional deliberations on FBI charter legislation.

The Seattle Police Intelligence Ordinance

The Seattle Intelligence Ordinance specifies that police may not collect restricted information without authorization by a commander of specified rank. Authorization may be granted in response to a written request from a prosecuting attorney, a city attorney, the Attorney General of the state, or the Attorney General of the United States. Conditions for the granting of the written authorization are spelled out

in the Ordinance, and a full specification of the necessary contents of the authorization is given. These include the identity of the subject; the violation of law, past or pending, to which the collection of restricted information is deemed relevant; an explanation of the restricted information sought and its relevance; the basis for a reasonable suspicion that the subject has engaged in or is about to engage in unlawful activity; justification for the use of an informant or infiltrator if one is to be used; and an explanation of protective measures to avoid violations of civil rights.

Extensions of up to 90 days may be authorized by the Chief of the Department. Additional authorizations must describe the restricted data already collected and justify the need to collect additional information. Restricted information received without an authorization must be purged.

The Ordinance defines the conditions that must be met for transmission of restricted information to another criminal justice or governmental agency and, in particular, to the County Prosecuting Attorney or the City Attorney in connection with a judicial proceeding. It prohibits the use of infiltrators except under authorization to collect restricted information and with the written approval of the Chief of the Department. The infiltrator must be reviewed by the Chief or his designee at the end of each authorization period. The Ordinance also contains the instructions to be given to paid informants in carrying out their assignment, and it itemizes the powers and functions of the Department's Criminal Intelligence Section, which processes and analyzes all investigative information.

The Ordinance provides for the appointment of an Auditor by the Mayor, subject to City Council confirmation, to conduct in-place audits of Department files and records at unscheduled intervals not exceeding 180 days to ascertain whether there have been any violations of the Intelligence Ordinance. Each final report of the Auditor, accompanied by written comments of the Chief, is forwarded to the Mayor, the City Council, the City Attorney, and the City Comptroller. The Chief must immediately investigate any violations reported. The Auditor has the further duty of notifying any person about whom restricted information may have been collected in violation of the Intelligence Ordinance and who may have a civil remedy.

Finally, the Ordinance sets forth civil liability of the City to persons whose rights have been injured by violation of its provisions and specifies minimum damages to be thereby payable. It also mandates an annual report by the Chief of the Department on its implementation, to be submitted to the Mayor, the City Council, and the City Controller and to be filed as a public record.

Proposed Operational Guidelines for the Los Angeles PDID

The Chief of Police, the Director of the Office of Special Services, the Commanding Officer of the PDID, or a PDID Section Officer in charge can direct the initiation of an investigation to furnish intelligence information, but the Commanding Officer of the PDID has the primary responsibility for ensuring compliance with the operational guidelines. The Legal Officer of the Division has the responsibility for continuously reviewing the procedures to ensure that they conform to current statutory and case law.

When PDID investigators collect raw information, they must evaluate the reliability, relevance, and accuracy of the material and then forward it to the Data Analysis Unit. The Unit screens the information and retains only that which meets specified reliability, relevance, and accuracy criteria. The Unit may make an estimate or projection concerning an event or situation on the basis of its analysis of the screened information.

When a PDID officer completes a preliminary investigation and the subject is shown to meet the Standards and Procedures criteria for inclusion in the PDID files, or when a PDID officer obtains additional qualifying information on a subject already in the files, the guidelines mandate the preparation of an Intelligence Report according to a strict procedure that involves review by the Section Supervisor, the Section Officer in Charge, the Commanding Officer of the PDID, and the Officer in Charge of the Research/Legal Unit. The Intelligence Report is then filed in a new or existing file package on the subject, and entries are made on a new or existing Vice/Intelligence file card on the subject.

The guidelines describe the preparation, routing, and storage of briefing reports used by the Commanding Officer of the PDID for weekly briefings of the Chief of Police and the Director of the OSS concerning past, current, and impending events that have public-disorder implications.

The guidelines also describe a special intelligence report, the Rumor Report, which records information about upcoming events or incidents that may require police action. Procedures for routing, approving, and storing Rumor Reports are specified to assist commanding officers in the deployment of police personnel.

The PDID must maintain an Inquiry/Dissemination Log of requests and responses to requests for information contained in PDID intelligence files. The entries in the log are based on individual Inquiry/Dissemination Reports that contain detailed data on the request and requestor, the requisite approvals for dissemination under the standards and procedures, and the nature of the information disseminated. Every member of the PDID is responsible for completing a weekly Liaison/Contact Report that classifies all contacts with persons outside the PDID into categories of organizations to which these persons belong.

In their present draft form, the guidelines touch lightly or not at all upon a number of matters that are addressed in the Attorney General's Guidelines and the Seattle Ordinance, including time limits and criteria for the termination of investigations and limitations on the techniques of gathering information.

Procedures for Public Security Activities of the NYPD

Controls on the initiation of Public Security investigations by the NYPD Intelligence Division have already been noted, along with the responsibility of the Commanding Officer of the Intelligence Division for authorizing supplementary investigations. In general, written Public Security reports originate in the analysis section and are based on screened and classified intelligence information. The Commanding Officer approves these reports and determines their distribution.

Public Security reports and communications are of three general types: (1) strategic/indicative, routed through the Commanding Officer of the Intelligence Division; (2) tactical/evidential, routed through

the appropriate operational command; or (3) informational/for file only, retained in Public Security files without distribution. The Commanding Officer is responsible for identifying reports that are unusually sensitive and should have separate storage, and for determining which files can be accessed only by the Commanding Officer, his Executive Officer, the Public Security Coordinator, or designated persons with a need to know.

In general, dissemination of information from any Public Security files intradepartmentally or to other governmental and law-enforcement agencies requires approval of the Commanding Officer of the Intelligence Division. He is also the sole approving authority for dissemination of surveillance photos, to which access is particularly limited.

The Intelligence Division Legal Officer is charged with the review of these guidelines to ensure their consonance with statutory and case law. The First Deputy Commissioner or his representative and the Commanding Officer of the Intelligence Division review all Public Security activities for compliance with the procedures specified in the guidelines.

Appendix A

THE ATTORNEY GENERAL'S GUIDELINES FOR FBI DOMESTIC SECURITY INVESTIGATIONS
(March 10, 1976)

I. Bases of Investigation

A. Domestic security investigations are conducted, when authorized under Section II(C), II(F), or II(I), to ascertain information on the activities of individuals, or the activities of groups, which involve or will involve the use of force or violation of federal law, for the purpose of:

1. overthrowing the government of the United States or the government of a State;

2. substantially interfering, in the United States, with the activities of a foreign government or its authorized representatives;

3. substantially impairing for the purpose of influencing U.S. government policies or decisions:
   (a) the functioning of the government of the United States;
   (b) the functioning of the government of a State; or
   (c) interstate commerce.

4. depriving persons of their civil rights under the Constitution, laws, or treaties of the United States.

II. Initiation and Scope of Investigations

A. Domestic security investigations are conducted at three levels--preliminary investigations, limited investigations, and full investigations--differing in scope and in investigative techniques which may be used.

B. All investigations undertaken through these guidelines shall be designed and conducted so as not to limit the full exercise of rights protected by the Constitution and laws of the United States.

Preliminary Investigations

C. Preliminary investigations may be undertaken on the basis of allegations or other information that an individual or

a group may be engaged in activities which involve or will involve the use of force or violence and which involve or will involve the violation of federal law for one or more of the purposes enumerated in IA(1)-IA(4). These investigations shall be confined to determining whether there is a factual basis for opening a full investigation.

D. Information gathered by the FBI during the preliminary investigations shall be pertinent to verifying or refuting the allegations or information concerning activities described in paragraph IA.

E. FBI field offices may, on their own initiative, undertake preliminary investigations limited to:

1. examination of FBI indices and files;
2. examination of public records and other public sources of information;
3. examination of federal, state, and local records;
4. inquiry of existing sources of information and use of previously established informants; and
5. physical surveillance and interviews of persons not mentioned in E(1)-E(4) for the limited purpose of identifying the subject of an investigation.

Limited Investigations

F. A limited investigation must be authorized in writing by a Special Agent in Charge or FBI Headquarters when the techniques listed in paragraph E are inadequate to determine if there is a factual basis for a full investigation. In addition to the techniques set forth in E(1)-E(4) the following techniques also may be used in a limited investigation:

1. physical surveillance for purposes other than identifying the subject of the investigation;
2. interviews of persons not mentioned in E(1)-E(4) for purposes other than identifying the subject of the investigation, but only when authorized by the Special Agent in Charge after full consideration of such factors as the seriousness of the allegation, the need for the interview, and the consequences of using the technique. When there is a question whether an interview should be undertaken, the Special Agent in Charge shall seek approval of FBI Headquarters.

G. Techniques such as recruitment or placement of informants in groups, "mail covers," or electronic surveillance, may not be used as part of a preliminary or limited investigation.

H. All preliminary and limited investigations shall be closed within 90 days of the date upon which the preliminary investigation was initiated. However, FBI Headquarters may authorize in writing extension of a preliminary or limited investigation for periods of not more than 90 days when facts or information obtained in the original period justify such an extension. The authorization shall include a statement of the circumstances justifying the extension.

Full Investigations

I. Full investigations must be authorized by FBI Headquarters. They may only be authorized on the basis of specific and articulable facts giving reason to believe that an individual or a group is or may be engaged in activities which involve the use of force or violence and which involve or will involve the violation of federal law for one or more of the purposes enumerated in IA(1)-IA(4). The following factors must be considered in determining whether a full investigation should be undertaken:

1. the magnitude of the threatened harm;
2. the likelihood it will occur;
3. the immediacy of the threat; and
4. the danger to privacy and free expression posed by a full investigation.

Investigative Techniques

J. Whenever use of the following investigative techniques are permitted by these guidelines, they shall be implemented as limited herein:

1. use of informants to gather information, when approved by FBI Headquarters, and subject to review at intervals not longer than 180 days; provided,

   (a) when persons have been arrested or charged with a crime, and criminal proceedings are still pending, informants shall not be used to gather information concerning that crime from the person(s) charged; and
   (b) informants shall not be used to obtain privileged information; and where such information is obtained by an informant on his own initiative no record or use shall be made of the information.

2. "mail covers," pursuant to postal regulations, when approved by the Attorney General or his designee, initially or upon request for extension; and

3. electronic surveillance in accordance with the requirement of Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

Provided that whenever it becomes known that person(s) under surveillance are engaged in privileged conversation (e.g., with attorney), interception equipment shall be immediately shut off and the Justice Department advised as soon as practicable. Where such a conversation is recorded it shall not be transcribed, and a Department attorney shall determine if such conversation is privileged.

NOTE: These techniques have been the subject of strong concern. The committee is not yet satisfied that all sensitive areas have been covered (e.g., inquiries made under "pretext," "trash covers," photographic or other surveillance techniques).

III. Terminating Investigations

A. Preliminary, limited, and full investigations may be terminated at any time by the Attorney General, his designee, or FBI Headquarters.

B. FBI Headquarters shall periodically review the results of full investigations, and at such time as it appears that the standard for a full investigation under II(1) can no longer be satisfied and all logical leads have been exhausted or are not likely to be productive, FBI Headquarters shall terminate the full investigation.

C. The Department of Justice shall review the results of full domestic intelligence investigations at least annually, and shall determine in writing whether continued investigation is warranted. Full investigations shall not continue beyond one year without the written approval of the Department. However, in the absence of such notification the investigation may continue for an additional 30 day period pending response by the Department.

IV. Reporting, Dissemination, and Retention

A. Reporting

1. Preliminary investigations which involve a 90-day extension under II(H) and limited investigations

under II(F) shall be reported periodically to the Department of Justice. Reports of preliminary and limited investigations shall include the identity of the investigation, the identity of the person interviewed or the person or place surveilled, and shall indicate which investigations involved a 90-day extension. FBI Headquarters shall maintain, and provide to the Department of Justice upon request, statistics on the number of preliminary investigations instituted by each field office, the number of limited investigations under II(F), the number of preliminary investigations that involved 90-day extensions under II(H), and the number of preliminary or limited investigations that resulted in the opening of a full investigation.

2. Upon opening a full domestic security investigation the FBI shall, within one week, advise the Attorney General or his designee thereof, setting forth the basis for undertaking the investigation.

3. The FBI shall report the progress of full domestic security investigations to the Department of Justice not later than 90 days after the initiation thereof, and the results at the end of each year the investigation continues.

4. Where the identity of the source of information is not disclosed in a domestic security report, an assessment of the reliability of the source shall be provided.

B. Dissemination

1. Other Federal Authorities
The FBI may disseminate facts or information obtained during a domestic security investigation to other federal authorities when such information:

(a) falls within their investigative jurisdiction;
(b) may assist in preventing the use of force or violence; or
(c) may be required by statute, interagency agreement approved by the Attorney General, or Presidential directive. All such agreements and directives shall be published in the Federal Register.

2. State and Local Authorities
The FBI may disseminate facts or information relative to activities described in paragraph I(A) to state and local law enforcement authorities when such information:

(a) falls within their investigative jurisdiction;
(b) may assist in preventing the use of force or violence; or
(c) may protect the integrity of a law enforcement agency.

3. When information relating to serious crimes not covered by paragraph I(A) is obtained during a domestic security investigation, the FBI shall promptly refer the information to the appropriate lawful authorities if it is within the jurisdiction of state and local agencies.

4. Nothing in these guidelines shall limit the authority of the FBI to inform any individual(s) whose safety or property is directly threatened by planned force or violence, so that they may take appropriate protective safeguards.

5. The FBI shall maintain records, as required by law, of all disseminations made outside the Department of Justice, of information obtained during domestic security investigations.

C. Retention

1. The FBI shall, in accordance with a Records Retention Plan approved by the National Archives and Records Service, within _____ years after closing domestic service investigations, destroy all information obtained during the investigation, as well as all index references thereto, or transfer all information and index references to the National Archives and Records Service.

NOTE: We are not yet certain whether empirical data exist to help define a period of retention for information gathered in preliminary or full investigations. Whatever period is determined should take into account the retention period for other categories of information (e.g., general criminal, organized crime, and background checks); since we have not yet considered these areas, we cannot fix a period for retention at this time.

NOTE: It may also be possible to establish a sealing procedure to preserve investigative records for an interim period prior to destruction. After being sealed, access would be permitted only under controlled conditions.

2. Information relating to activities not covered by paragraph I(A) obtained during domestic security investigations, which may be maintained by the FBI

under other parts of these guidelines, shall be retained in accordance with such other provisions.

3. The provisions of paragraphs one (1), and two (2) above apply to all domestic security investigations completed after the promulgation of these guidelines, and apply to investigations completed prior to promulgation of these guidelines when use of these files serves to identify them as subject to destruction or transfer to the National Archives and Records Service.

4. When an individual's request pursuant to law for access to FBI records identifies the records as being subject to destruction or transfer under paragraph one (1), the individual shall be furnished all information to which he is entitled prior to destruction or transfer.

Appendix B

THE ATTORNEY GENERAL'S GUIDELINES FOR FBI USE OF INFORMANTS IN DOMESTIC SECURITY, ORGANIZED CRIME, AND OTHER CRIMINAL INVESTIGATIONS

(December 15, 1976)

TO: Clarence M. Kelley
Director
Federal Bureau of Investigation

FROM: Edward H. Levi
Attorney General

Courts have recognized that the government's use of informants is lawful and may often be essential to the effectiveness of properly authorized law enforcement investigations. However, the technique of using informants to assist in the investigation of criminal activity, since it may involve an element of deception and intrusion into the privacy of individuals or may require government cooperation with persons whose reliability and motivation may be open to question, should be carefully limited. Thus, while it is proper for the FBI to use informants in appropriate investigations, it is imperative that special care be taken not only to minimize their use but also to ensure that individual rights are not infringed and that the government itself does not become a violator of the law. Informants as such are not employees of the FBI, but the relationship of an informant to the FBI imposes a special responsibility upon the FBI when the informant engages in activity where he has received, or reasonably thinks he has received, encouragement or direction for that activity from the FBI.

To fulfill this responsibility, it is useful to formulate in a single document the limitations on the activities of informants and the duties of the FBI with respect to informants, even though many of these

limitations and duties are set forth in individual instructions or recognized in existing practice.

As a fundamental principle, it must be recognized that an informant is merely one technique used in the course of authorized investigations. The FBI may not use informants where it is not authorized to conduct an investigation nor may informants be used for acts or encouraged to commit acts which the FBI could not authorize for its undercover Agents. When an FBI informant provides information concerning planned criminal activity which is not within the investigative jurisdiction of the FBI, the FBI shall advise the law enforcement agency having investigative jurisdiction. If the circumstances are such that it is inadvisable to have the informant report directly to the agency having investigative jurisdiction, the FBI, in cooperation with that agency, may continue to operate the informant.

A. Use of Informants

In considering the use of informants in an authorized investigation, the FBI should weigh the following factors--

1. the risk that use of an informant in a particular investigation or the conduct of a particular informant may, contrary to instructions, violate individual rights, intrude upon privileged communications, unlawfully inhibit the free association of individuals or the expression of ideas, or compromise in any way the investigation or subsequent prosecution.
2. the nature and seriousness of the matter under investigation,

and the likelihood that information which an informant could provide is not readily available through other sources or by more direct means.

3. the character and motivation of the informant himself; his past or potential involvement in the matter under investigation or in related criminal activity; his proven reliability and truthfulness or the availability of means to verify information which he provides.
4. the measure of the ability of the FBI to control the informant's activities insofar as he is acting on behalf of the Bureau and ensure that his conduct will be consistent with applicable law and instructions.
5. the potential value of the information he may be able to furnish in relation to the consideration he may be seeking from the government for his cooperation.

B. Instructions to Informants

The FBI shall instruct all informants it uses in domestic security, organized crime, and other criminal investigations that in carrying out their assignments they shall not:

1. participate in acts of violence; or
2. use unlawful techniques (e.g., breaking and entering, electronic surveillance, opening or otherwise tampering with the mail) to obtain information for the FBI; or
3. initiate a plan to commit criminal acts; or
4. participate in criminal activities of persons under investigation, except insofar as the FBI determines that such

participation is necessary to obtain information needed for purposes of federal prosecution.

Whenever the FBI learns that persons under investigation intend to commit a violent crime, informants used in connection with the investigation shall be instructed to try to discourage the violence.

C. Violations of Instructions and Law

1. Under no circumstances shall the FBI take any action to conceal a crime by one of its informants.

2. Whenever the FBI learns that an informant used in investigating criminal activity has violated the instructions set forth above in furtherance of his assignment, it shall ordinarily notify the appropriate law enforcement or prosecutive authorities promptly of any violation of law, and make a determination whether continued use of the informant is justified. In those exceptional circumstances in which notification to local authorities may be inadvisable, the FBI shall immediately notify the Department of Justice of the facts and circumstances concerning the investigation and the informant's law violation, and provide it recommendation on reporting the violation and on continued use of the informant. The Department shall determine:

(a) when law enforcement or prosecutive authorities should be notified of the law violation;

(b) what use, if any, should be made of the information

gathered through the violation of law, as well as the disposition and retention of such information; and

(c) whether continued use should be made of the informant by the FBI.

Note: Since the FBI has a special responsibility to control the activity of informants collecting information for the Bureau, and is ordinarily familiar with these activities, a comparatively minimal degree of certainty on the part of the FBI (e.g., "learns") is required before the FBI must report informant misconduct to the appropriate law enforcement authorities.

3. Whenever the FBI has knowledge of the actual commission of a serious crime by one of its informants unconnected with his FBI assignment, it shall ordinarily notify the appropriate law enforcement or prosecutive authorities promptly and make a determination whether continued use of the informant is justified. In those exceptional circumstances in which notification to local authorities may be inadvisable, the FBI shall promptly advise the Department of Justice of the facts and circumstances concerning the investigation and the informant's law violation, and provide its recommendation on reporting the violation and on continued use of the informant. The Department of Justice shall determine:

(a) when law enforcement or prosecutive authorities should be notified of the law violation; and

(b) whether continued use should be made of the informant by the FBI.

Note: Because the criminal activity described in this provision is independent of any government assignment, and since the FBI will have no special knowledge to determine such informant malfeasance, a substantial degree of certainty on the part of the Bureau is required before it must report to other authorities. The standard of certainty is derived from the federal Misprison of Felony statute, 18 U.S.C. 4, "Whoever, having knowledge of the actual commission of a felony cognizable by a court of the United States, conceals and does not as soon as possible make known the same to some judge or other person in civil or military authority under the United States, shall be fined not more than $500 or imprisoned not more than three years, or both."

4. In determining the advisability of notifying appropriate law enforcement and prosecutive authorities of criminal activity by FBI informants the FBI and the Department of Justice shall consider the following factors:

   (a) whether the crime is completed, imminent or inchoate;

   (b) seriousness of the crime in terms of danger to life and property;

   (c) whether the crime is a violation of federal or state law, and whether a felony, misdemeanor or lesser offense;

   (d) the degree of certainty of the information regarding the criminal activity;

(e) whether the appropriate authorities already know of the criminal activity and the informant's identity; and

(f) the significance of the information the informant is providing, or will provide, and the effect on the FBI investigative activity of notification to the other law enforcement agency.

Appendix C

SUMMARY AND SELECTED PROVISIONS OF THE FREEDOM OF INFORMATION ACT[1]

The Freedom of Information Act, which Congress enacted in 1966 and amended in 1974, mandates Federal agencies to make available to the public all information held by them save for that falling within one of nine exceptions. (See 5 U.S.C. Sec. 552(b) below.) All agency opinions, orders, and rules are included and must be made generally available for public inspection and copying. An order that is not properly indexed and made available to the public may not even be relied upon or cited as precedent by an agency.

The Act contains no provision forbidding disclosure; the exemptions protect against required disclosure, not against disclosure. The question of disclosure of information in one or more of the exempt categories is left to the discretion of an agency.

Any person, including corporations, partnerships and other associations as well as individuals, may request identifiable records from an agency in accordance with procedures established and published by that agency. If access is denied for any reason, the requestor may bring suit in Federal district court where he resides, or has his principal place of business, or where the records are located. The court has jurisdiction to order the agency to show that the records need not be produced. If the court's order for disclosure is not complied with, the responsible agency employee may be held in contempt. The Act

[1]The summary borrows mainly from two references: Singleton and Hunter, op. cit., pp. 52-55; "FOIA and Privacy Act Interface," op. cit., pp. 570-572.

provides that FOIA lawsuits have precedence on court calendars.

The impact of the Act is specifically on subdivisions of the executive branch and their employees. A person or institution which contracts to perform services for the government does not thereby become subject to all requirements of the FOIA. Individual government officials such as the Attorney General and the FBI Director are subject to the FOIA. A claim that disclosure is unduly burdensome is no excuse, courts have ruled, even though the burden may justify some delay.

Procedurally, given a request which reasonably describes the records sought and which conforms to the agency's published rules, an agency must determine within ten working days whether the requested material falls within one or more of the exceptions. If the request is refused, both initially and after administrative appeal, then the requestor has standing to sue in Federal district court to compel the disclosure of the material. The court determines the mattter de novo, with the burden of proof on the agency to justify denial. The court may examine the contested material in secret and determine whether any reasonably segregable portion must be disclosed. Beyond this injuction to disclose, no other remedies, civil or criminal, are provided by the Act.

Generally, the courts have been permissive in deciding who is entitled to seek information under the FOIA, and usually the identity of the persons for whom the records are sought need not be revealed to the agency.

5 U.S.C. Sec. 552(b)

(b) This section does not apply to matters that are--

(1)(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;

(2) related solely to the internal personnel rules and practices of an agency;

(3) specifically exempted from disclosure by statute (other than section 552b of this title) provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(7) investigatory records compiled for law enforcement purposes, but only to the extent that the production of such records would (A) interfere with enforcement proceedings, (B) deprive a person of a right to a fair trial or an impartial adjudication, (C) constitute an unwarranted invasion of personal privacy, (D) disclose the identity of a confidential source and, in the case of a record compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, confidential information furnished only by the confidential source, (E) disclose investigative techniques and procedures, or (F) endanger the life or physical safety of law enforcement personnel;

(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for

the use of an agency responsible for the regulation or supervision of financial institutions; or

Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection.

5 U.S.C. Sec. 552(e)

(e) For purposes of this section, the term "agency" as defined in section 551(1) of this title includes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency.

Appendix D

SUMMARY AND SELECTED PROVISIONS OF THE PRIVACY ACT OF 1974[1]

The Privacy Act of 1974 attempts to safeguard personal privacy by limiting the collection, maintenance, use, and dissemination of personal information by Federal agencies. The Act covers all executive departments, the military, independent regulatory agencies, government corporations, and government-controlled corporations. It does not apply to Congress, the Federal courts, the District of Columbia, or the government of U.S. territories or possessions. Its substance includes the following:

Agency Requirements

Each agency must publish annually in the Federal Register a notice of the existence and character of its records systems.

In collecting information for its records systems, each agency is required to give the following facts to each individual asked to supply information: (1) its authority; (2) whether supplying the information is voluntary or mandatory; (3) consequences of refusal to supply; (4) purpose for which the information is to be used; and (5) routine uses which may be made of the information. Each agency is required to collect information to the greatest extent practicable for the individual concerned.

[1]The summary borrows from "Protecting Privacy from Government Invasion: Legislation at the Federal and State Levels," op. cit., pp. 783-791.

Each agency may store only such information about an individual as is relevant and necessary to accomplish a required purpose of the agency. Records used in making determinations about an individual must be maintained with such accuracy, relevancy, timeliness, and completeness as is reasonably necessary to insure fairness. An agency may not, with certain exceptions, maintain records describing an individual's exercise of First Amendment rights. In addition to these limitations on the type of information which may be maintained, the Act imposes requirements as to the security of records kept by agencies.

Agencies are forbidden to disclose any record contained in a system of records except by written consent or upon request of the individual who is the subject of the record. Disclosures may, however, be made without prior consent in eleven circumstances. (See 5 U.S.C.a(b) quoted below.) Before disseminating any individual's record to a person other than an agency, each agency must make reasonable efforts to insure that such records are accurate, timely, and relevant for agency purposes.

Agencies must keep an accurate accounting of the date, nature, and purpose of each disclosure of a record, and of the name and address of the person or agency to whom the disclosure is made. Such accounting must be kept for at least five years and must be made available to the individual named in the request.

Rights of Individuals

An individual who is the subject of a record has the right to gain access to his record and to copy it, upon request. The individual may also request amendment of a record which pertains to him. Within ten

days of the receipt of such a request, the agency involved must acknowledge the receipt of the request in writing. It must then correct the record, or inform the individual of its refusal to amend the record pursuant to his request, stating the reason for refusal and the procedures for review of the refusal. If the individual seeks review, the final agency determination must usually be made within thirty working days. If the reviewing official also refuses to amend the record, the individual must be notified of the provisions for judicial review. If the agency refuses to amend, the individual is allowed to file a statement setting forth the reasons for his disagreement. Subsequent disclosures must be accompanied by copies of the statement and a notation indicating disputed portions of the record. Also, notice about any correction or notation of dispute must be given to any person or agency to whom the record was previously disclosed.

Exemptions

The Act permits exemptions from many of its provisions if the system of records is maintained by the CIA. The same exemptions are allowed for other law enforcement agencies if the record system consists of (1) information compiled for purposes of identifying individual criminal offenders; (2) information compiled for purposes of a criminal investigation; or (3) reports on an individual compiled at any law enforcement stage. (See 5 U.S.C. 552(j) quoted below.) More specific exemptions, applicable mainly to the access and challenge provisions, may be established for seven other classes of records. (See 5 U.S.C. 552(k) quoted below.) These exemptions are permissive rather than

mandatory; the head of the agency must promulgate a rule to obtain the exemption.

Remedies

An agency may be sued civilly in Federal district court in four situations: (1) refusal to grant an individual access to his records; (2) refusal to amend an individual's records pursuant to his request, or failure to review that refusal; (3) failure to maintain an accurate, relevant, timely, and complete record which results in a determination adverse to the individual; and (4) failure to comply with any other provision of the Act or of a rule promulgated thereunder so as adversely to affect the individual. The district court may order the agency to amend the individual's record or to produce a record. It may assess attorney's fees and costs against the United States. Where the individual prevails and the court determines the agency action was intentional or willful, the United States will be liable for the actual damages, which may not be less than $1,000 plus attorney's fees and costs.

A misdemeanor conviction and a maximum fine of $5,000 are provided as criminal penalties in three situations: (1) when any officer or employee of an agency knowingly discloses information in violation of the Act; (2) when any officer or employee maintains a system of records without meeting the notice requirements of the Act; or when any person knowingly or willfully requests or obtains a record concerning an individual under false pretenses.

5 U.S.C. Sec. 552a(b)

(b) Conditions of disclosure.--No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be--

(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

(2) required under section 552 of this title;

(3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;

(4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;

(5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

(6) to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Administrator of General Services or his designee to determine whether the record has such value;

(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;

(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;

(9) to either House of Congress, or, to the extent of

matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;

(10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office; or

(11) pursuant to the order of a court of competent jurisdiction.

5 U.S.C. 552a(j)

(j) General exemptions.--The head of any agency may promulgate rules, in accordance with the requirements (including general notice)of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i) if the system of records is--

(1) maintained by the Central Intelligence Agency; or

(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section

553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

5 U.S.C. 552a(k)

(k) Specific exemption.--The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3) (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H) and (I) and (f) of this section if the system of records is--

(1) subject to the provisions of section 552(b)(1) of this title;

(2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: Provided, however, that if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18;

(4) required by statute to be maintained and used solely as statistical records;

(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the

identity of the source would be held in confidence;

(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or

(7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

Comments by the Privacy Protection Study Commission[2]

"Although all Federal agency record-keeping operations that fit the Privacy Act's definition of a system of records are subject to some of its requirements, the Act's scope of application is significantly narrowed by the opportunity it gives some agencies to exempt whole systems from many of the Act's more important requirements. This is particularly true of systems maintained for law enforcement and investigative purposes. Subsection 3(j) of the Act permits exemption from most requirements if the records in a system of records are records maintained by the Central Intelligency Agency (5 U.S.C. 552a(j)(1)); or identification files, investigative records, or records compiled on

[2]"Exempt Systems of Records," The Privacy Act of 1974: An Assessment, Appendix 4 to the Report of the Privacy Protection Study Commission, July 1977, pp. 7-8.

individuals during the time between arrest and final release and maintained by an agency 'or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws' (5 U.S.C. 552a(j)(2)). The provisions of the Act from which records cannot be exempted under subsection 3(j) are primarily those that establish certain records management responsibilities. For example, an accounting of disclosures of information from an exempt system must be kept, and an agency that maintains an exempt law enforcement system must be kept, and an agency that maintains an exempt law enforcement system must take steps to assure the accuracy and relevance of records it discloses to anyone other than an agency, but the basic oversight and enforcement vehicles otherwise available in the Act, i.e., individual access and correction remedies, cannot be used to make sure the agency complies.

"The exemption opportunities in subsection 3(k) (5 U.S.C. 552a(k)) are less sweeping than those in subsection 3(j), but they also serve to insulate many systems from fundamental protections the Act elsewhere guarantees an individual. Subsection 3(k)(2) creates an exemption opportunity for investigatory records compiled from both criminal and civil law enforcement purposes that have not already qualified for an exemption under subsection 3(j)(2). An agency that takes a 3(k)(2) exemption for a system of records is excused from granting an individual access to records about himself; from revealing to the individual its accounting of disclosures it makes of records about him; from publishing certain portions of the required annual notice about the system; and from promulgating regulations establishing procedures by which the

individual can see, copy, and correct or amend a record about himself. Subsection 3(k), like subsection 3(j), also allows an exemption from the Act's requirement that the information in a system be 'relevant and necessary' to accomplish a purpose mandated by law. . . ."

Appendix E

DISCOVERY IN CRIMINAL PROCEEDINGS

The discovery process in a criminal proceeding is an avenue by which domestic security intelligence held by government agencies may suffer disclosure. This appendix briefly reviews the fundamentals of criminal discovery, emphasizing its relevance to intelligence disclosure. It is in three main parts, namely: (1) description of criminal discovery in Federal courts; (2) consideration of the Freedom of Information Act, viewed as a complement to traditional criminal discovery; and (3) description of criminal discovery in California courts, with brief mention of comparable matters in Florida, New York, and Illinois for contrast.

FEDERAL CRIMINAL DISCOVERY[1]

Discovery within Federal criminal proceedings is founded on court rules of procedure, case decisions, and statutes.

Pretrial discovery by the defense is governed primarily by Rule 16 of the Federal Rules of Criminal Procedure.[2] Rule 16 is supplemented by Rule 7(f),[3] which provides for a defense motion to obtain a bill of particulars, and by a line of Supreme Court decisions of which Brady v. Maryland[4] is the leading case--decisions that compel government disclosure of certain evidence helpful to the defendant. These rules and decisions are the legal foundation for the transmission of material information from the government to the defendant before trial. On the other hand, the Jencks Act[5] is a statutory tool that enables the defense to obtain certain information from the government during trial.

Concerning Rule 16

Rule 16(a) provides that, upon request of the defendant, the government shall:

---

[1]A primary reference for this and the following section is W. Jordan, W. Kehoe, and R. Schecter, "The Freedom of Information Act--A Potential Alternative to Conventional Criminal Discovery," Note, American Criminal Law Review, v. 14, Summer 1976.

[2]Rule 16 is reproduced in full at the end of this appendix.

[3]Rule 7(f) is as follows: "The court may direct the filing of a bill of particulars. A motion for a bill of particulars may be made before arraignment or within ten days after arraignment or at such later time as the court may permit. A bill of particulars may be made before arraignment or within ten days after arraignment or at such later time as the court may permit. A bill of particulars may be amended at any time subject to such conditions as justice requires."

[4]373 U.S. 83 (1963).

[5]18 U.S.C. Sec. 3500 (Supp. I, 1970).

- o permit him to inspect and to copy written, recorded or oral statements that he has made--as a matter of right subject only to the possibility of a protective order under 16(d)(1), Rule 16(a)(1)(A));
- o furnish him a copy of his prior criminal record, Rule 16(a)(1)(B));
- o permit him to inspect and to copy documents and tangible objects within the possession and control of the government, which are either material to his defense; or are intended to be prosecutorial evidence; or are derived from him, Rule 16(a)(1)(C));
- o permit him to inspect and to copy any results or reports of physical or mental examinations, and of scientific tests or experiments that are material to the defense or are intended for use by the government as evidence, Rule 16(a)(1)(D)).

The most proximate to intelligence disclosure of the above items is Rule 16(a)(1)(C). It enables a defendant to discover government-held documents and tangible objects if he can show that they are material to his defense; or that they were obtained from or belong to him; or that the government intends to use them as evidence.[6] However, Rule 16(a)(2) precludes discovery of "reports, memoranda, or other internal government documents made by . . . government agents in connection with

[6]The language is sufficiently broad to require disclosure by the U.S. Attorney of evidence in the custody of another Federal agency.

the investigation or prosecution of the case, . . ." unless discovery is provided for by (1)(A), (1)(B), or (1)(D). This "work product" rule appears to shield domestic security intelligence files generated for the case at hand, but not other intelligence documents that are material to the defense. In any event, under Rule 16(d)(1), provided that the government makes a "sufficient showing" for a protective order, the court has the power to deny discovery otherwise allowed by Rule 16.

Rule 16(c) imposes a continuing duty to disclose on the government. It provides that the defendant must be promptly notified about additional discoverable material that was the subject of an earlier discovery request, once the government obtains knowledge of the existence of th material.

Rule 16(d)(2) specifies various sanctions available to the trial court if there is a failure to comply with its discovery order. The court may prohibit the introduction of evidence not disclosed, may grant a continuance, or "may enter such other order as it deems just under the circumstances." If the government denies discovery of materials that the court deems essential to a fair rial, it is undoubtedly within the court's discretion to dismiss the proceedings.

The government, in turn, is allowed a limited amount of discovery by Rule 16, namely, if it has complied with a discovery request under 16(a)(1)(C) or (D), then it is permitted to inspect and to copy papers, documents, tangible objects, etc., that the defendant intends to introduce as evidence. But there is a "work product" exemption applicable to discovery by the government.

Concerning Rule 7(f)

The motion for a bill of particulars is not important to the issue of intelligence disclosure. A motion for a bill of particulars should be made by the defendant when he is confronted with a vague or confusing indictment or information. The purpose of the bill is to supply details sufficient to enable the defendant to prepare for trial and to minimize the danger of surprise at trial. It is well established by case decisions that the bill is not designed to force the government to disclose its evidence or its theory of the case. It is not, therefore, a mechanism of disclosure of domestic security intelligence.

Concerning the Brady v. Maryland Duty of Disclosure

The U.S. Supreme Court has held that in some instances a denial of discovery to a defendant is a denial of due process. Indeed, in certain cases, the prosecutor has an affirmative duty to disclose to the defendant evidence that might exculpate him. In the words of the Court, as expressed in Brady: ". . . suppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material either to guilt or to punishment, irrespective of the good faith or the bad faith of the prosecutor." The test of materiality is whether the evidence would affect the outcome of the trial.

More narrowly, the Supreme Court ruled in a case that preceded Brady that the government had no absolute right not to disclose the identity of an informant.[7] The Court said: "Where the disclosure of

[7]Rovario v. United States, 353 U.S. 53 (1957).

an informer's identity . . . is relevant and helpful to the defense of an accused . . . the privilege must give way." It called for a balancing of the public interest in protecting the flow of information against the accused's right to prepare his defense, in other words, a case-by-case determination of disclosure or nondisclosure of an informant's identity.[8]

Brady and related decisions left unanswered a number of questions about the scope of the disclosure requirement. For example, the time at which the defendant is entitled to inspect evidence favorable to him is not specified--some courts have favored pretrial disclosure; others disclosure at trial. It is not settled whether a defense request is a necessary prerequisite, nor is it clear how specific a defense request

---

[8]The following points about the disclosure of informant identity are made in an authoritative source. It is settled law that the Government has a privilege of refusing to disclose the identity of its informants at trial. The Supreme Court recognizes that there is no fixed disclosure rule and that disclosure must depend upon the particular circumstances of each case, taking into consideration the crime charged, the possible defense, the possible significance of the informant's testimony, and other relevant factors.

A mere request for disclosure is generally held to be insufficient. Defense counsel must clearly present the grounds for seeking disclosure. The extent of the informant's participation in the crime charged is a significant factor in deciding whether his identity should be disclosed. The Supreme Court expects district judges to scrutinize with great care the Government's refusal to reveal the identity of an informant and, when properly advised as to the need for disclosure, to mandate it. Where the defendant makes a showing that his participation in the crime resulted from entrapment by the informant, disclosure is required. However, where the Government's proof at trial is able to establish defendant's predisposition to commit the crime to a conclusive degree, the legal error in the Government's failure to disclose the informant's identity may be found harmless in appellate review. Where information supplied by an informant is the only source of probable cause for an arrest without a warrant, disclosure of his identity will be compelled. Proving Federal Crimes, Sixth Edition, prepared by the Criminal Division of the Office of the U.S. Attorney for the Southern District of New York, April 1976.

must be. Importantly, the Supreme Court has not decided what is the depth of the disclosure requirement, beyond its holding that any category of information shown to be material to either guilt or punishment is subject to disclosure. For example, in Giles v. Maryland,[9] the Court left open the issue whether the prosecutor must disclose "all evidence admissible and useful to the defense." Thus, the impact of the Brady disclosure duty on domestic security intelligence files cannot be fully perceived.

Concerning the Jencks Act

Since the Jencks Act, which provides for defense access to statements made by a government witness which relate to the subject matter of his testimony at trial, is not central to the issue of intelligence disclosure, we need not dwell on its use here. These discovery rights arise only after a government witness has testified on direct examination during trial.

Recapitulation

Two aspects of Federal criminal discovery have been identified as particularly relevant to the disclosure of domestic security intelligence information. One is Rule 16(a)(1)(C) as limited by Rule 16a(2), the effect of which is to preclude the discovery of such intelligence records generated in connection with the criminal charges being tried, but not the discovery of intelligence materials produced otherwise yet material to the defense. The government would have to

[9]386 U.S. 66 (1967).

make a "sufficient showing" to deny discovery of the latter. The other is disclosure mandated by Brady when the intelligence information is material to either guilt or punishment, including disclosure of informant identity.

THE FOIA AS A DISCOVERY MECHANISM IN FEDERAL CRIMINAL PROCEEDINGS.

The FOIA requires Federal agencies (as defined in the Act) to make their records promptly available to any person who requests them, unless they fall within one of nine narrowly construed exemptions. Futhermore, the Act provides that any reasonable segregable portion of a record requested shall be provided after deletion of the portions which are exempt.

In the sense that the scope of the FOIA is confined to "records," it is narrower than the scope of criminal discovery. Moreover, courts have not fully settled the meaning of "record" for the purposes of the FOIA. Certainly, physical evidence and unrecorded oral statements--potentially discoverable materials in a criminal case--are not records. But since domestic security intelligence files appear clearly to be records, this difference between conventional discovery and FOIA discovery is of little consequence.

Another aspect of the scope of the FOIA (as a discovery mechanism in Federal criminal proceedings) is the extent of material exempted from disclosure. The seventh exemption is of dominant importance as respects the disclosure of domestic security intelligence information. Its language, as amended in 1974, exempts:

> investigatory records compiled for law enforcement purposes, but only to the extent that the production of such records would (A) interfere with law enforcement proceedings, (B) deprive a person of a right to a fair trial or an impartial adjudication, (C) constitute an unwarranted invasion of privacy, (D) disclose the identity of a confidential source, and in the case of a record compiled by a law enforcement agency in the course of a criminal investigation, confidential information furnished only by a confidential source, (E) disclose investigative techniques and procedures, or (F) endanger the life or physical safety of law enforcement personnel.

There will be no review here of the court decisions that contain interpretations of the language of the seventh exemption--most of which focuses on harms (A) and (D) specified above. Instead, what may be emphasized is that the seventh exemption does not per se shield domestic security intelligence information from disclosure. Depending upon what is requested under the FOIA, this information--with possibly some deletions due to the seventh exemption--might be obtained by the defense.

Advantages and disadvantages of the FOIA as a discovery mechanism, in comparison with conventional crime discovery, will be briefly recounted below. But these points should be viewed not as if the FOIA is in fact a substitute for the usual discovery approach.[10] Rather, the FOIA should be regarded as a possibly useful complement, mainly serving to fill gaps of information and to reach records not normally

---

[10]There are special situations in which the use of traditional discovery is unavailable or unwise and in which the use of the FOIA as a discovery mechanism would not be merely complementary. For example, normal discovery cannot be invoked before criminal charges are filed, but FOIA rights of access can be pursued nonetheless. Another example: Defense counsel may be deterred from making a discovery motion under Rule 16 because the government would gain reciprocal discovery rights as a result.

discoverable. It should be noted that some distinctions made below are being eroded, for example, by the decision in U.S. v. Brown, 562 F.2d 1144 (CA9 Wash., 1977). In Brown, a defendant requested records from a Federal agency (the Bureau of Prisons) under Rule 16(a)(1)(C) by right of access under the FOIA. (The normal procedure for an FOIA request would have been that specified in the Code of Federal Regulations by the agency involved.) The Court of Appeals decided that the defendant's discovery procedure was proper and that the trial court in the criminal proceeding was the appropriate tribunal for judicial review of the agency's denial of the FOIA request. In other words, Brown says that no separate civil action challenging nondisclosure under the FOIA is required (at least in the Ninth Circuit). This case resolves the issue of whether a court with criminal jurisdiction is empowered to enforce a defendant's rights under the FOIA; but it avoids the issue of whether the civil court in the FOIA matter would enjoin the prosecution of the criminal case until an FOIA order for disclosure is met.

Advantages of FOIA Discovery

There are several procedural advantages in FOIA discovery as compared with conventional discovery. One concerns the timing of the discovery request. An FOIA request can be made at any time, and an FOIA civil action can be filed once the agency has reviewed its denial or has failed to meet the FOIA time limits for its initial response or for its denial review.[11] By contrast, conventional criminal discovery motions

[11]The FOIA specifies as follows:

"Each agency, upon any request for records made under paragraph (1), (2), or (3) of this subsection, shall--

must be filed within the period set by the court rules, usually between arrest and a specified post-arraignment date.

Another procedural advantage has to do with standing required to make a request. "Any person" is entitled to information under the FOIA. By contrast, in traditional discovery, the requestor is necessarily the defendant, and his ability to require disclosure depends upon a showing of a certain relationship, for example, as specified in Rule 16(a) or as satisfying a Brady claim, between his case and the materials requested.

Still another procedural advantage is that a criminal defendant does not carry the burden in an FOIA request of proving that the material should be disclosed. By contrast, in an ordinary discovery motion, he must show that the information sought is relevant, that the request is reasonable, and that the information is within the scope of discovery.

Finally, there is the matter of judicial discretion. Once a court has determined that material requested under the FOIA is not protected

---

(i) determine within ten days (excepting Saturdays, Sundays, and legal public holidays) after the receipt of any such request whether to comply with such request and shall immediately notify the person making such request of such determination and the reason therefore, and of the right of such person to appeal to the head of the agency any adverse determination; and

(ii) make a determination with respect to any appeal within twenty days (excepting Saturdays, Sundays, and legal public holidays) after the receipt of such appeal. If on appeal the denial of the request for records is in whole or in part upheld, the agency shall notify the person making such request of the provisions for judicial review of that determination under paragraph (4) of this subsection." (a)(6)(A)

Under unusual circumstances, as defined in (a)(6)(B), either of the above time limits can have an extension not exceeding ten working days. Thus, a minimum lapse of 30 to 50 working days could be expected between the making of an FOIA request and the filing of a civil action for judicial review of its denial.

by a specific exemption, it has rarely exercised its equitable powers to withhold this information. By contrast, courts have exercised considerable discretion in dealing with traditional discovery requests; and only an abuse of discretion will lead to reversal on appeal.

The main substantive advantage of an FOIA request is, of course, its potential for reaching information (in government hands) whose disclosure cannot be compelled by an ordinary discovery motion. For example, it is within the trial judge's discretion to order disclosure of the prosecutor's witness list in response to a discovery motion, but courts do not generally accede to such requests. Witness lists appear to be available to the criminal defendant under the FOIA in some, if not most, cases.

Further targets for an FOIA request by a criminal defendant would be policy guidelines formulated within a U.S. Attorney's Office, which direct the legal position an individual prosecutor should assume under specified case facts; workbooks describing the procedural route for implementing a chosen legal position on a case; and statistical files that describe the decisional pattern of the prosecutor's office. There are highly complex considerations involved in the determination of whether or not specific instances of such materials must be disclosed under the FOIA. They will not be reviewed here. But it may be noted that very substantial releases of this kind of information have resulted from FOIA requests.

Disadvantages of FOIA Discovery

Since the FOIA was not designed to be a discovery tool for criminal proceedings, it is not surprising that troublesome delays and expense, as

well as inadequate remedies, might be encountered in its use for this purpose. But we have noted--for example, in U.S. v. Brown--developments that help to alleviate these disadvantages.

Under the FOIA an agency is entitled to at least 30 working days (or possibly as many as 50 working days in special circumstances) in which to respond to a request. If it denies the request, the agency has 30 days in which to answer the complaint in an FOIA suit. So, several months can easily pass before an information request is resolved when an agency opts to resist.

It could turn out that the use of the FOIA as a discovery tool is expensive in terms of copying costs, attorney's fees, and litigation costs. (The Brown decision, however, points to a means of ameliorating this disadvantage.) Of course, if the criminal defendant's request prevails, the court may assess against the government resonable attorney's fees and other litigation costs.

Remedies for the failure of the government to comply with its disclosure duty are more limited in the FOIA setting than in traditional criminal discovery. In an FOIA case the court can order the production of any agency record improperly withheld and, in the event of noncompliance with the order, the court may punish for contempt the responsible employee. It is doubtful that a judge in an FOIA civil matter would enjoin the prosecution of the criminal case from which the request stemmed until his FOIA order had been met. By contrast, the Federal Rules of Criminal Procedure accord a trial judge broad discretion in dealing with failure to comply with a discovery order. He may prohibit the introduction of the evidence not disclosed, grant a

continuance of the trial, or "enter such other order as [he] deems just under the circumstances," possibly including a dismissal.

Finally, the government has no continuing duty to produce additional material after an FOIA request has been filled, although a court could issue an order requiring the agency to provide any document within a specified period, for example, before the end of the proceeding. Under Rule 16(c) of the Rules of Criminal Procedure, the government has a continuing duty to disclose additional evidence previously requested or ordered.

Put plainly, the FOIA has enlarged the potential for discovery in a Federal criminal proceeding. Domestic security intelligence is neither more nor less vulnerable to disclosure by an FOIA request because the latter is prompted by a criminal proceeding. Yet a criminal proceeding is a powerful incentive to initiate and pursue an attempt to have such information disclosed.

CRIMINAL DISCOVERY IN CALIFORNIA AND ELSEWHERE[12]

It was not until 1956 that the California Supreme court first clarified that a criminal defendant is entitled to discover items of evidence in the possession or under the control of the prosecution. Although the Legislature in 1957 enacted comprehensive statutory provisions governing discovery in civil actions, no such statutes have been enacted concerning discovery in criminal proceedings--but there are

[12]The sources here are standard legal reference works including 18 Cal Jur--Criminal Law (1975, supp. 1979); 13A Bender's Forms of Discovery--Criminal Discovery (1967, rev. 1979); and 4B California Forms of Pleading and Practice--Criminal Procedure (1972, cum. supp. 1979).

some specific provisions, for example, Penal Code Sec. 1430 (1975) provides that upon the defendant's first court appearance, the prosecuting attorney must make available within two calendar days copies of the police, arrest, and crime reports (with privileged information deleted). In the words of the Supreme Court, authority for discovery is derived "not from statute but from the inherent power of every court to develop rules of procedure aimed at facilitating the administration of criminal justice and promoting the orderly ascertainment of truth."

California courts have ruled on five general types of evidentiary items that are discoverable on a proper showing by the defendant as follows:

(1) Prior statements made by him to police or prosecution authorities;

(2) Statements made by a codefendant or an alleged conspirator to police or prosecution authorities;

(3) Names and addresses known to the prosecution of eyewitnesses to the crime with which the defendant is charged and photographs of him exhibited to the victim for purposes of identificaion;

(4) Statements made by prospective[13] prosecution of eyewitnesses to police or prosecution authorities as well as prior felony convictions and sexual offenses of prosecution witnesses when material;

(5) Physical evidence in the possession of the prosecution as

[13]Note that this provision is more liberal than the Federal provision under the Jencks Act.

> well as reports of the state's experts concerning such physical evidence.

In addition, statutory law (Evidence Code Sec. 1042(d)) provides that the prosecution in a criminal action must disclose the identity of a police informer if the court concludes that there is a reasonable possibility that nondisclosure might deprive the defendant of a fair trial.

The fundamentals of California discovery in criminal proceedings are captured in the following succinct summary, borrowed from a standard legal treatise:[14]

> Pretrial discovery rights in criminal cases have been developed by court decision. Pretrial discovery in favor of defendants is based on the fundamental principle that an accused is entitled to a fair trial and is permitted to promote orderly ascertainment of the truth. The accused may, before trial, inspect and copy statements of his own in the prosecutions's possession as well as statements of persons expected to be prosecution witnesses. And the prosecution may, in a proper case, be compelled to make available to the accused real evidence in its possession. Where otherwise proper, the accused may compel the prosecution to disclose the identity of an informant.... The trial court's refusal to order pretrial discovery as requested by the accused may be reviewed on appeal from a judgment of conviction. Mandamus lies to compel pretrial production of evidentiary material improperly withheld in a criminal case. And a writ of prohibition may issue to restrain the court from enforcing an improper pretrial discovery order. (Section references omitted.)

While California criminal discovery on its face does not appear to reach significantly farther than Federal criminal discovery, its being largely court-fashioned is conducive to growth, particularly as respects the discovery of sensitive information in the files of law enforcement

---

[14]18 Cal Jur--Criminal Law, p. 672.

agencies.[15] An impressive example is the case of Murgia v. Municipal Court, 15 Cal.3d 286 (1975), where the California Supreme Court ruled that a defense of deliberate invidious discrimination in law enforcement could be maintained and that, on the basis of this defense, defendants were entitled to an order directing the prosecutor to produce information, including police records, relevant to the claim of discriminatory law enforcement.

The scope of criminal discovery varies widely among the states--in some, it is more limited than Federal criminal discovery; in others, much broader.[16] Two of the states in which interviews of criminal justice officials and ex-officials were conducted for the purposes of this study illustrate relative extremes in criminal discovery, namely, Florida and New York.

---

[15]Of course, since some aspects of criminal discovery in California are governed by statute, the courts have their usual role of interpreting what the Legislature commands. For example, in a recent case, People v. Hertz, 80 Daily Journal D.A.R. 873 (C.A.2d, March 25, 1980), the Court of Appeal dealt with an ambiguity in Evidence Code Section 915, pertaining to judicial in camera review of material that a public agency refuses to disclose on the grounds of its privilege to withhold "official information" whose revelation is against the public interest. Here defendants sought to discover, among other things, certain information in police intelligence files, which was then claimed by the police to be privileged official information. The magistrate held an in camera proceeding prior to the preliminary hearing, to determine the validity of the claim of privilege. He disallowed the presence of a court reporter to transcribe the proceeding, based on his interpretation of an ambiguity in the relevant Evidence Code provisions. The trial court dismissed the criminal charges against the defendants in part because of the failure of the magistrate to create a reviewable record of the in camera proceedings during discovery hearings. The Court of Appeal upheld the dismissals, thereby expanding the law of criminal discovery.

[16]This discussion draws from 13A Bender's Forms of Discovery, Appendix A--Criminal Discovery, Appendix--81.

Within its Rules of Criminal Procedure, Florida has enacted Rule 3.220, Discovery, perhaps the most liberal in the nation. While similar to Federal Rule 16, it is much more detailed and comprehensive. This rule provides, for example, that after the filing of the indictment or information, within 15 days after written demand by the defendant, the prosecutor must disclose almost everything material to the criminal proceedings within the prosecutor's knowledge, except work product and possibly the identity of confidential informants. (Disclosure of a confidential informant is not required unless the latter is to be produced at a hearing or trial, or a failure to disclose his identity will infringe the constitutional rights of the accused.) Disclosure duties are also imposed on the defendant in return for the prosecutor's compliance with Rule 3.220. Both parties have continuing duties to disclose. The court has power to deny or regulate disclosures upon a showing of cause, which may be made in camera upon a request of a party. Florida has not only accepted the Jencks Act rationale, but has expanded it to the extent that a defendant may examine statements of a prospective witness before trial. The disclosure of any material information within the state's possession or control which tends to negate the guilt of the accused must be made as soon as practicable after the filing of the indictment or information whether or not a request is made by the defendant. Police personnel records may be discovered upon a showing of materiality to the preparation of the defense.

In Florida, violation by the state of Rule 3.220 does not call for reversal of conviction unless the record discloses that such noncompliance resulted in prejudice or harm to the defendant. Also, the

burden is on the defendant to show why the disclosure of the identity of a confidential informant should be compelled.

New York, on the other hand, has not developed a full-fledged doctrine of criminal discovery. It does not provide for pretrial discovery of objects or documents which are not in themselves admissible in evidence, nor does it even require automatic inspection of the defendant's own confession.

Specifically, upon motion by a defendant, the court must order discovery of the defendant's record of testimony before the grand jury, and of a written or recorded statement made by the defendant to law enforcement personnel, which materials are within the possession or control of the district attorney. The court may order discovery of reports and documents concerning physical and mental examinations or scientific tests and experiments in connection with the case if within the district attorney's possession or control. This order may be conditioned on reciprocal discovery granted to the prosecution. Either order may be vacated, restricted, or qualified upon a sufficient showing in opposition to the discovery motion. Similarly, the court may order discovery of other property designated by the defendant and within the possession or control of the district attorney provided the defendant shows that such property is material to the preparation of his defense and that his discovery request is reasonable. New York rules exempt from discovery work product and also records of statements made to either side by witnesses or prospective witnesses in the case. Both sides have a continuing duty to disclose.

New York has adopted the Jencks Act rationale and does mandate that once a witness has testified under direct examination, any prior statement he has made, whether before the grand jury or to the police, is discoverable in full without prior inspection by the trial court. The law is unclear, however, as to whether a document which may be in part confidential may be inspected by the defense. It is presumed that in such case the Jencks Act provision for trial court inspection will be invoked.

Illinois, another state in which our interviews were conducted, provides for broad discovery of material and information under the state's control once an indictment or information has been filed (similar to Florida law). The fact that the Illinois discovery rules are not operative prior to or in the course of a preliminary hearing has given rise to an Illinois Supreme Court decision, People ex rel. Fisher v. Carey, 77.I11.2d 259 (Oct. 1979), expanding access by defense counsel. In this case the Court decided the issue of whether a subpoena duces tecum may issue for normally discoverable police reports before the determination of probable cause but after an accused has been "charged" or "booked." It ruled in the affirmative, holding that such subpoenaed material must be delivered to the court for screening as to privilege; and the State's Attorney may not intercept and screen these materials, but is not barred from seeing what has been subpoenaed. Its decision rests on the principle that a subpoena is a judicial process that is statutorily and constitutionally independent of discovery rules; and that defense counsel should not be barred from any formal recourse to evidence gathering until after a determination of probable cause.

EXTRACT FROM FEDERAL RULES OF CRIMINAL DISCOVERY

RULE 16. DISCOVERY AND INSPECTION

(a) Disclosure of Evidence by the Government

(1) Information Subject to Disclosure

(A) Statement of Defendant. Upon request of a defendant the government shall permit the defendant to inspect and copy or photograph: any relevant written or recorded statements made by the defendant, or copies thereof, within the possession, custody or control of the government, the existence of which is known, or by the exercise of due diligence may become known, to the attorney for the government; the substance of any oral statement which the government intends to offer in evidence at the trial made by the defendant whether before or after arrest in response to interrogation by any person then known to the defendant to be a government agent; and recorded testimony of the defendant before a grand jury which relates to the offense charged. Where the defendant is a corporation, parnership, association or labor union, the court may grant the defendant, upon its motion, discovery of relevant recorded testimony of any witness before a grand jury who (1) was, at the time of his testimony, so situated as an officer or employee as to have been able legally to bind the defendant in respect to conduct constituting the offense, or (2) was, at the time of the offense, personally involved in the alleged conduct constituting the offense and so situated as an officer or employee as to have been able legally to bind the defendant

in respect to that alleged conduct in which he was involved.

(B) Defendant's Prior Record. Upon request of the defendant, the government shall furnish to the defendant such copy of his prior criminal record, if any, as is within the possession, custody, or control of the government, the existence of which is known, or by the exercise of due diligence may become known, to the attorney for the government.

(C) Documents and Tangible Objects. Upon request of the defendant the government shall permit the defendant to inspect and copy or photograph books, papers, documents, photographs, tangible objects, buildings or places, or copies or portions thereof, which are within the possession, custody or control of the government, and which are material to the preparation of his defense or are intended for use by the government as evidence in chief at the trial, or were obtained from or belong to the defendant.

(D) Reports of Examinations and Tests. Upon request of a defendant the government shall permit the defendant to inspect and copy or photograph any results or reports of physical or mental examinations, and of scientific tests or experiments, or copies thereof, which are within the possession, custody, or control of the government, the existence of which is known, or by the exercise of due diligence may become known, to the attorney for the government, and which are material to the preparation of the defense or are intended for use by the government as evidence in chief at the trial.

(2) Information Not Subject to Disclosure. Except as provided in paragraphs (A), and (B), and (D) of subdivision (A)(1), this rule does not authorize the discovery or inspection of reports, memoranda, or other internal government documents made by the attorney for the government or other government agents in connection with the investigation or prosecution of the case, or of statements made by government witnesses or prospective government witnesses except as provided in 18 U.S.C. 3500.

(3) Grand Jury Transcripts. Except as provided in Rule 6 and subdivision (a)(1)(A) of this rule, these rules do not relate to discovery or inspection of recorded proceedings of a grand jury.

(4) Failure to Call Witness. The fact that a witness' name is on a list furnished under this rule shall not be grounds for comment upon a failure to call the witness.

(b)Disclosure of Evidence by the Defendant.

(1) Information Subject to Disclosure.

(A) Documents and Tangible Objects. If the defendant requests disclosure under subdivision (a)(1)(C) or (D) of this rule, upon compliance with such request by the government, the defendant, on request of the government, shall permit the government to inspect and copy or photograph books, papers, documents, photographs, tangible objects, or copies or portions thereof, which are within the possession, custody, or control of the defendant and which the defendant intends to introduce as evidence in chief at the trial.

(B) Reports of Examinations and Tests. If the defendant requests disclosure under subdivision (a)(1)(C) or (D) of this rule, upon compliance with such request by the government, the defendant, on request of the government, shall permit the government to inspect and copy or photograph any results or reports of physical or mental examinations and of scientific tests or experiments made in connection with the particular case, or copies thereof, within the possession or control of the defendant, which the defendant intends to introduce as evidence in chief at the trial or which were prepared by a witness whom the defendant intends to call at the trial when the results or reports relate to his testimony.

(2) Information Not Subject to Disclosure. Except as to scientific or medical reports, this subdivision does not authorize the discovery or inspection of reports, memoranda, or other internal defense documents made by the defendant, or his attorneys or agents in connection with the investigation or defense of the case, or of statements made by the defendant, or by government or defense witnesses, to the defendant, his agents or attorneys.

(3) Failure to Call Witness. The fact that a witness' name is on a list furnished under this rule shall not be grounds for comment upon a failure to call a witness.

(c) Continuing Duty to Disclose. If, prior to or during trial, a party discovers additional evidence or material previously requested or ordered, which is subject to discovery or inspection under this rule, he shall promptly notify the other party or his attorney or the court of the existence of the additional evidence or material.

(d) Regulation of Discovery.

(1) Protective and Modifying Orders. Upon a sufficient showing the court may at any time order that the discovery or inspection be denied, restricted, or deferred, or make such other order as is appropriate. Upon motion by a party, the court may permit the party to make such showing, in whole or in part, in the form of a written statement to be inspected by the judge alone. If the court enters an order granting relief following such an ex parte showing, the entire text of the party's statement shall be sealed and preserved in the records of the court to be made available to the appellate court in the event of an appeal.

(2) Failure to Comply With a Request. If at any time during the course of the proceedings it is brought to the attention of the court that a party has failed to comply with this rule, the court may order such party to permit the discovery or inspection, grant a continuance, or prohibit the party from introducing evidence not disclosed, or it may enter such other order as it deems just under the circumstances. The court may specify the time, place and manner of making the discovery and inspection and may prescribe such terms and conditions as are just.

(e) Alibi Witnesses. Discovery of alibi witnesses is governed by Rule 12.1.

As amended Feb. 28, 1966, eff. July 1, 1966; Apr. 22, 1974, eff. Dec. 1, 1975; July 31, 1975, Pub.L. 94-64 3(20)-(28), 89 Stat. 374, 375.

RAND/N-1902-DOJ INTELLIGENCE CONSTRAINTS OF THE 1970s AND DOMESTIC TERRORISM: VOL. II, A SURVEY OF LEGAL, LEGISLATIVE, AND ADMINISTRATIVE CONSTRAINTS M. Lavin